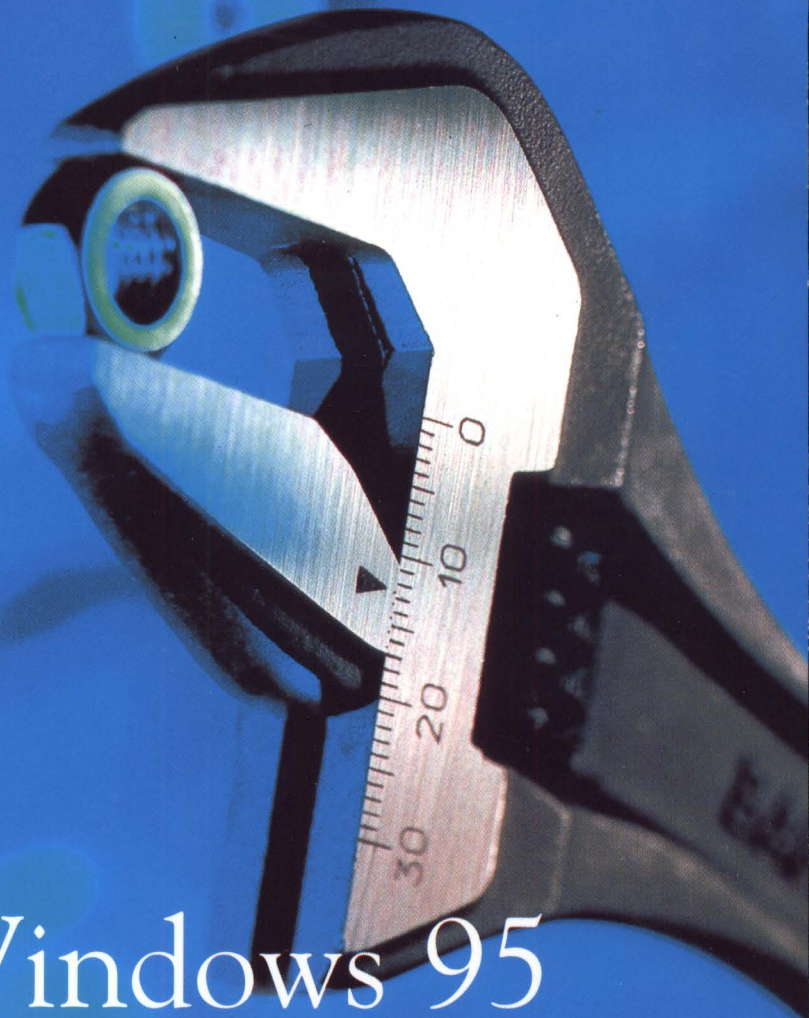
DR SOLOMON'S

Anti-Virus Toolkit



Windows 95

Dr Solomon's
Anti-Virus Toolkit
for Windows 95

Dr Solomon's Software Ltd.
Alton House, Gatehouse Way, Aylesbury, Buckinghamshire, HP19 3XU, UK
Tel: +44 (0)1296 318700 Fax: +44 (0)1296 318777
E-mail: support@uk.drsolomon.com

Dr Solomon's Software, Inc.
1 New England Executive Park, Burlington, MA 01803, USA
Tel: +1 617 273 7400 Fax: +1 617 273 7474
E-mail: support@us.drsolomon.com

Dr Solomon's Software GmbH
Luisenweg 40, 20537 Hamburg, Deutschland
Telefon: +49 (0)40 2519 54-0 Fax: +49 (0)40 2519 54-50
E-mail: support@de.drsolomon.com

CompuServe: GO DRSOLOMON
World Wide Web: http://www.drsolomon.com/

SS1117A-20-05

Copyright

Dr Solomon's Anti-Virus Toolkit for Windows 95 is copyright © 1996 Dr Solomon's Software Ltd. All rights reserved. Dr Solomon's Anti-Virus Toolkit for Windows 95 is not copy-protected. This does not mean that you can make unlimited copies of it. Dr Solomon's Anti-Virus Toolkit for Windows 95 is protected by the copyright laws which pertain to computer software. It is illegal to make copies of the program other than as may be licensed or for purposes of backup without written permission from Dr Solomon's Software Ltd. No part of the manual or other documentation accompanying Dr Solomon's Anti-Virus Toolkit for Windows 95 may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language, in any form or by any means, without the prior written permission of Dr Solomon's Software Ltd.

Disclaimer

Neither Dr Solomon's Software Ltd. nor anyone else who has been involved in the creation, production or delivery of Dr Solomon's Anti-Virus Toolkit for Windows 95 or this manual makes any warranties with respect to the contents of the software or this manual and each specifically disclaims any implied warranties to the extent allowed by legislation. Dr Solomon's Software Ltd. reserves the right to revise the software and the manual and to make changes from time to time in the contents without obligation to notify any person.

Trademarks

Dr Solomon's is a registered trademark of Dr Solomon's Software Ltd. All other product names mentioned are acknowledged to be the marks of their producing companies.

Software release

This manual describes version 7.6 of Dr Solomon's Anti-Virus Toolkit for Windows 95.

Manual edition

Edition 1.2

October 1996

Quickstart

If you need to act quickly, read the next two pages, especially if you think you may have a virus.

If you have bought the Toolkit because you suspect you might have a virus, the most important things to remember are:

- Don't panic.
- Don't rush into anything.

You could end up causing more damage than the virus.

Quick virus check

If you are anxious to perform a check for viruses as quickly as possible, you can run FindVirus without installing the Toolkit, as follows:

1. Switch off the PC.
2. Insert a virus-free, write-protected, DOS system diskette in the A drive and switch on the PC.

   Ideally, you should use the system diskette that was supplied with your PC.
3. When the system prompt appears, insert the diskette containing FINDVIRU.EXE from the DOS Toolkit into the drive. This is usually, but not always, the diskette labelled Toolkit DOS Disk 2. You can use the DIR command to check.
4. Change to that drive by typing `A:` or `B:` as appropriate and pressing ↵ .
5. Type `FINDVIRU /LOCAL`. Press ↵ .

   FindVirus scans your local drives for viruses. If it finds a virus, it displays the virus name on the screen.

Quick Repair

If you do have a virus, the simplest way to remove it is as follows:

1. Boot from a clean, write-protected, DOS system diskette.
2. At the system prompt, insert the diskette containing FINDVIRU.EXE from the DOS Toolkit into the appropriate drive.
3. Change to that drive by typing `A:` or `B:` and pressing ↵ .
4. Type `FINDVIRU /REPAIR /LOCAL` and press ↵ .
5. The screen displays a list of the files infected. Where possible, files are repaired, otherwise they are renamed.

   If the boot sector of a diskette is infected, it is replaced with a clean boot sector.

Contents

Preface ..... **vii**
How to use this manual vii
Conventions ix
What you need ix
Using the keyboard x
Short-cut keys x
Key functions xi
Related documentation xi
Windows & DOS Anti-Virus Toolkit manual xi
The Virus Encyclopedia xi
Other versions of the Anti-Virus Toolkit xii
Registration and upgrades xiii
If you need help xiv

1. Introduction **1**
1.1 What is a virus? 1
1.2 Types of virus 3
File viruses 3
Macro viruses 4
Boot and partition sector viruses 4
Companion viruses 5
Overwriting viruses 5
Multipartite viruses 5
Droppers 6
The future 6
1.3 Characteristics of viruses 6
Stealth 6
Polymorphism 6
Virus names 7
Variants 7
How viruses spread 7
1.4 Other potential problems 8
Bugs 8
Low-level software clashes 9
Trojans 9
Time bombs and logic bombs 10
Jokes 10
Human Error 10
1.5 What you can do 11
Backups 11
Software sources 12

Diskettes and other media 12
Employee co-operation 13
1.6 The Anti-Virus Toolkit 13
FindVirus 13
VirusGuard 14
WinGuard 14
ViVerify 14
The Virus Encyclopedia 15

2. Installing the Toolkit 17
2.1 How to install the Toolkit 17
WinGuard 19
VirusGuard 19
Installing the Scheduler 21
Completion of installation 22
2.2 README files 23
2.3 How to uninstall the Toolkit 23
2.4 Upgrading the Toolkit 24

3. Finding your Way Around 25
3.1 Starting the Toolkit 25
3.2 The main screen 27
3.3 Options on the menus 28
File menu 28
Scan menu 29
Repair menu 29
Advanced menu 30
Help menu 30

4. Guarding against Viruses 31
4.1 Using WinGuard 32
Configuring WinGuard 32
Advanced features of WinGuard 36
If WinGuard reports a virus 36
4.2 Using VirusGuard 37
How VirusGuard uses memory under DOS 37
If VirusGuard reports a virus 38

5. Checking for Viruses 39
5.1 Finding Viruses - FindVirus 39
When to use FindVirus 39
Running FindVirus from the main screen 40
Running FindVirus from the Scan menu 41
FindVirus advanced options 42

If FindVirus reports a virus 44
5.2 Inspecting disks and files 45
Inspect disk 45
Inspect file 47
5.3 Checking for changes - ViVerify 49
When to use ViVerify 50
Running ViVerify 50
To compute the fingerprints 52
Checking the files 53
If a file has changed 53
Advanced menu options 54
5.4 The Virus Encyclopedia 56

6. Virus Repair and Removal 59
6.1 If you find a Virus 59
6.2 Single button repair 61
6.3 If you discover a new virus 62
6.4 Repair menu options 64
Repairing drive 64
Replacing diskette boot sectors 65
6.5 Shredding files 67
6.6 Eradicating a virus 68
Planning the clean-up 68
Checking diskettes 69
Checking PCs 69

7. Using the Scheduler 71
7.1 The Schedule Editor 71
7.2 To set up a new event 73
Setting the event details 74
Scan settings 75
Frequency settings 77
7.3 Running the Scheduler 78
7.4 Managing the event file 78
7.5 The Toolkit Event Log 79
7.6 Setting up Scheduler defaults and options 79
General defaults 80
Scan Settings 81
List Boxes 82

8. Advanced Virus Detection 83
8.1 How FindVirus works 83
Executable files 84
Compressed and archived files 84
Repairing files 85

8.2 Running FindVirus from the user interface 86
8.3 Running FindVirus from the command line 86
Syntax 86
Scanning specific drives 88
Scanning files and folders 89
Scanning boot and partition sectors 91
Producing reports 91
Identifying viruses 92
Specifying actions 93
Defining drivers 93
Repairing files 94
Scanning backup files 95
False alarms 95
8.4 Error messages 95

9. Advanced Virus Prevention 97
9.1 How VirusGuard works 97
Running VirusGuard 97
Use of memory 98
Security levels 99
Executable files 99
Boot sector scans 100
Finding viruses 100
9.2 Running VirusGuard 101
Scanning files when copying or reading 101
Scanning files when writing 102
Changing the pop-up message 104
9.3 Hints and Tips 105
Changing the security level 105
9.4 Testing VirusGuard 106
File virus test 106
Boot sector virus test 108
9.5 VirusGuard error messages 109

10. Advanced Virus Checking 111
10.1 How ViVerify works 111
Executable files 111
Encryption algorithms 112
Checking speed 112
Running ViVerify 113
10.2 Running ViVerify from the user interface 113
10.3 Running ViVerify from the command line 113
Syntax 113
Checking specific drives 115
Defining drives to be checked 115

Specifying a fingerprint file 116
Checking files 116
Checking boot and partition sectors 116
Specifying a keyword 116
Varying the checking speed and security 117
Specifying an algorithm 117
Defining actions 118
Producing reports 118

11. Toolkit Configuration 119
11.1 The TOOLKIT.INI file 119
FindVirus 120
FileRepair 120
ViVerify 121
11.2 Configuration File Management 121

12. Reference Information 123
12.1 FINDVIRU command 123
Syntax 123
Switches 123
12.2 GUARD command 125
Syntax 125
Switches 125
12.3 VIVERIFY command 126
Syntax 126
Switches 126
12.4 CLEANBOO command 127
Syntax 127
Switches 127
12.5 WTKUTIL command 128
Syntax 128
Switches 128
Commands 128

Glossary 131

Index 137

Preface

Dr Solomon's Anti-Virus Toolkit for Windows 95 contains everything you need to detect viruses, repair files and help prevent virus infection on your PC.

How to use this manual

This manual includes information for anyone using the Anti-Virus Toolkit for Windows 95, from the non-technical user to the PC expert. The sections you are interested in will depend on your level of knowledge and the information you need.

Chapters 1 and 2 are important for all readers. They provide background information on viruses and explain how to install the Toolkit.

Chapters 3 to 7 cover how to use the user interface and explain in detail the most straightforward ways to search for viruses and repair infected files.

Chapters 8 to 12 are aimed at more technical users. Read these if you want more in-depth information; for example, if you want to configure the tools for your particular needs.

If you do not have time to read the whole manual, particularly if you think you have a virus, read the Quickstart pages at the front of this manual.

Chapter 1 - Introduction explains what computer viruses are and the damage they can do. It explains the resources available in the Anti-Virus Toolkit to detect and remove viruses.

Chapter 2 - Installing the Toolkit gives step-by-step instructions for installing the Toolkit on your PC.

Chapter 3 - Finding Your Way Around shows you how to run the Toolkit programs, and explains the options that are available from each of the menus.

Chapter 4 - Guarding against Viruses describes the two memory-resident scanning programs that continually monitor disk and file accesses.

Chapter 5 - Checking for Viruses explains how to use the Toolkit to search for viruses on hard disks and diskettes.

Chapter 6 - Virus Repair and Removal explains the straightforward steps necessary to remove viruses and repair infections.

Chapter 7 - Using the Scheduler explains how you can set up virus checks and other programs to run at pre-set times.

Chapter 8 - Advanced Virus Detection provides detailed information on scanning for viruses using FindVirus.

Chapter 9 - Advanced Virus Prevention provides detailed information on intercepting viruses using VirusGuard.

Chapter 10 - Advanced Virus Checking provides detailed information on checking for changes in files using ViVerify.

Chapter 11 - Toolkit Configuration gives an explanation of the configuration files and how you can set them up and manage them.

Chapter 12 - Reference Information provides detailed information on the command line syntax and the switches for all the Toolkit commands.

A glossary is provided at the end of the manual, covering all the important terms used. There is also a comprehensive subject index.

Conventions

Throughout this manual, a number of conventions are used.

Information that you have to type is shown in the `Courier` typeface, for example:

```
WFINDV32 /LOCAL /DOALLFILES
```

Keys that you have to press are shown in the following form:

↓ Esc

↵ is used to indicate the Return or Enter key.

Throughout the text, symbols appear in the margin to draw your attention to particular points. These are as follows:

This indicates important information or tips to which you should pay particular attention.

This indicates a warning, and you should read it carefully.

What you need

The Anti-Virus Toolkit for Windows 95 runs on any PC running Windows 95.

Approximately 5 MB disk space is required.

If you want to install the Toolkit on more than one PC, you should enquire about a site licence from Dr Solomon's Software, or your local international distributor if you are outside the UK.

The Anti-Virus Toolkit for Windows 95 can detect all types of viruses. However, it cannot repair boot and partition sectors of hard disks. You need to reboot the system under DOS and run the Anti-Virus Toolkit for DOS. Therefore, for complete protection, the DOS Toolkit is also provided. See separate documentation for details.

You must have available a clean (that is, virus-free), write-protected, DOS system diskette (boot diskette). This could be the DOS system diskette supplied with your PC. You can then start up your computer from that diskette as part of the procedure for removing a virus infection.

It can be helpful if your clean system diskette also holds certain other files, namely:

- SYS.COM
- FDISK.COM

If you are using a disk compression or similar utility, you will also need the appropriate drivers on the system diskette.

Using the keyboard

Since Windows 95 was designed to be used with a mouse, it is strongly recommended that you use a mouse. However, all functions can be accessed from the keyboard if required.

Short-cut keys

Most Windows menu options can be selected by pressing short-cut key combinations, which are underlined.

Short-cut keys can always be used by pressing Alt + the short-cut key. For example, from the Toolkit user interface, pressing Alt + S displays the Scan drop-down menu.

Key functions

The keys that can be used within the Toolkit are as follows:

Key or combination	Function
↵	To accept a highlighted option button. The default button is normally OK.
Esc	To abandon a screen and return to the previous display.
Tab	To move to the next option in a dialog box.
Shift + Tab	To move to the previous option in a dialog box.
↓ ↑	Within a list of options, to move up and down the list.
Space	To select more than one item from a list.
F1	To display a screen of help text relevant to what you are doing.
Pg dn	To scroll down within the help text.
Pg up	To scroll up within the help text.

Related documentation

Windows & DOS Anti-Virus Toolkit manual

In certain circumstances you will need to use the DOS Toolkit provided. Instructions for this are in the Windows and DOS Anti-Virus Toolkit manual.

The Virus Encyclopedia

Included with your Toolkit is a copy of the Virus Encyclopedia book. As well as giving background information about viruses, it includes details of many of the viruses that the Toolkit can detect. The Encyclopedia categorizes each virus, describes its effects and

explains how it can be removed. It also lists any alternative names by which the virus is known.

An on-line version of the Virus Encyclopedia is also included in the Toolkit. As new viruses are found, they are included in the latest Toolkit upgrade. The on-line version will always be more up-to-date than the printed copy.

Other versions of the Anti-Virus Toolkit

Windows and DOS

The Windows and DOS version of the Anti-Virus Toolkit provides virus detection, repair and protection facilities for all PCs running Windows 3.x or DOS 3.1 or above.

Windows NT

The Windows NT version of the Anti-Virus Toolkit provides virus detection, repair and protection facilities for all Intel-based PCs running Windows NT.

Novell NetWare

The NetWare version of the Anti-Virus Toolkit provides tools to protect NetWare servers from viruses. For complete protection, the package also includes the DOS/Windows version of the Toolkit.

OS/2

There are now specific viruses which can infect OS/2 systems. The Anti-Virus Toolkit for OS/2 provides full protection for OS/2 systems, detecting OS/2, DOS and Windows viruses. The package also includes the full DOS version of the Toolkit.

SCO UNIX

The SCO UNIX version of the Anti-Virus Toolkit provides virus detection, repair and protection facilities for PCs running SCO UNIX. The package includes the DOS version of the Toolkit.

Apple Macintosh

The Apple Macintosh version of the Anti-Virus Toolkit provides virus detection, repair and protection facilities for machines running the MacOS.

Registration and upgrades

You will find a user registration card inside the Toolkit licence envelope. Complete the details on the card and return it to Dr Solomon's or the representative in your country. If you do not register your purchase you will not receive upgrades to the Toolkit.

If you cannot find the registration card, call Dr Solomon's or the representative in your country and quote the serial number on installation disk 1 of the Toolkit.

The virus researchers at Dr Solomon's constantly receive specimens of new viruses for investigation, and the Toolkit is upgraded each month to take account of these. Typically, between 100 and 150 new viruses are reported every month. If your Toolkit is out-of-date, a message appears on the screen when you run the software, to remind you to upgrade.

For your own protection you should therefore subscribe to the regular software upgrade service. For many people, a quarterly upgrade offers sufficient protection, but if your system is at particular risk or if security is of major importance, monthly upgrades are also available.

You may have purchased a Toolkit with a pre-paid subscription for the first year of upgrades. In this case, once you register you will automatically be sent monthly or quarterly upgrades for 12 months from the date on the card.

If you don't send us the card, you will not receive the upgrades that you have already paid for.

If you didn't buy a pre-paid subscription, send the appropriate amount when you return your registration card. Full details are given on the card.

Send in your registration card.

If you need help

If you have a problem while installing or running the Toolkit, there are a number of ways in which you can obtain help.

Check the documentation carefully, including any README files on the disks as well as this manual and the help text. Make sure you have installed the software correctly. Your authorized distributor may also be able to advise you.

If you still cannot solve the problem, Dr Solomon's support staff are available to help you. This service is free of charge.

You can contact Dr Solomon's Software by any of the following methods:

UK Office

By telephone:	+44 (0)1296 318700
By fax:	+44 (0)1296 318734
By e-mail:	support@drsolomon.com
By bulletin board:	+44 (0)1296 318810
By post:	Dr Solomon's Software Ltd. Alton House Gatehouse Way Aylesbury Buckinghamshire HP19 3XU United Kingdom

US Office

By telephone:	+1 617 273 7400
By fax:	+1 617 273 7474
By e-mail:	support@us.drsolomon.com
By bulletin board:	+1 617 229 8804
By post:	Dr Solomon's Software, Inc. 17 New England Executive Park Burlington MA 01803 USA

German Office

By telephone:	+49 (0)40 2519 54-0
By fax:	+49 (0)40 2519 54-50
By e-mail:	support@de.drsolomon.com
By post:	Dr Solomon's Software GmbH Luisenweg 40 20537 Hamburg Deutschland

World Wide

CompuServe:	GO DRSOLOMON
World Wide Web:	http://www.drsolomon.com/

When you contact Dr Solomon's, it is helpful to have the following information available:

- Your name and company.
- Your serial number as printed on installation disk 1 of the Toolkit.
- The version of Windows 95 you are using.
- The version number of the Toolkit you are using (this is printed on the label of the installation diskettes).
- A clean (virus-free), write-protected, DOS system diskette.
- In the case of an application error, any error messages reported.

If possible, you should be at the particular PC when you call us. We may need additional information, or we may ask you to carry out some diagnostic tests.

This page has been left blank.

1. Introduction

Computer viruses are a growing problem. When Dr Solomon's Software published the first version of the Anti-Virus Toolkit in 1989, the number of viruses at large in the world was in single figures. A year later, there were 50, and in the following year there were 200. By October 1995 there were over 7000. Between 100 and 150 new viruses are reported each month.

Many people panic when they hear the word *virus*. Remember though, computer viruses can be prevented, and if a virus infection is caught early it need not be particularly disruptive. The more preventative measures you can take the better, but you also need to be able to deal with a virus outbreak.

Dr. Solomon's Anti-Virus Toolkit for Windows 95 will detect viruses and deal with virus infections. It detects and removes any known virus, that is, known in the current version of the driver file.

This manual also gives you some useful guidelines for establishing an anti-virus policy and for dealing with an outbreak, should one occur.

1.1 What is a virus?

Computer viruses are so-called because they copy themselves. There are other types of software that can cause problems on your PC, and some of these are discussed in "Other potential problems" on page 8. However, no other type of software can replicate and it is this characteristic which makes a program a virus.

A virus is usually designed to copy itself without your knowledge. For example, it may attach itself to the FORMAT program and run every time you format a diskette.

If viruses do nothing but copy themselves, why are they such a problem?

Firstly, most viruses have deliberate or accidental side effects. Some of these seem harmless - they may simply display a message, make letters fall from the screen or play a tune. Others are specifically designed to be destructive, overwriting selected data or deleting files from the hard disk. In addition, many viruses do not operate as their authors intended them to because of bugs in the software; the side effects of these viruses are unpredictable. From the user's point of view, it does not matter whether the damage caused by a virus was a deliberate act by the virus author or an error in the program. Very few viruses were designed with Windows 95 in mind.

Secondly, most viruses stay in your PC's memory where they can cause problems by interfering with other software. Windows 95 normally prevents this.

Thirdly, once you have a virus, it is very likely that you will unwittingly pass it on to a colleague or a customer, who may well lose confidence in you and your company.

The majority of current viruses were designed to run under DOS. Many viruses use DOS-specific functions to operate and take advantage of undocumented DOS features that have been removed in Windows 95.

No virus is completely harmless; they all waste your time, processor time, memory and disk space. Dr. Solomon's Anti-Virus Toolkit for Windows 95 can help ensure that your PC remains free from such disruption and from virus infection.

1.2 Types of virus

The different types of virus, and the damage they can do, are outlined below.

File viruses

File viruses infect executable program files; these may include some data files containing executable macros. These usually, but not always, have COM or EXE file extensions. When you run an infected program the virus runs first, then passes control to the original program. While it has control, the virus code copies itself to another file or to another disk, replicating itself.

On Windows 95 systems, a file virus can run whenever a DOS application is run, either within a DOS box, or by running a DOS or 16-bit Windows executable file. Most file viruses try to go memory resident when they run. This attempt to become memory resident is likely to fail as memory is handled differently under Windows 95. This will severely hamper the viruses' ability to spread. So, will viruses die out? No, because underneath Windows 95 an implementation of DOS still exists. When you start your PC, DOS is run before Windows 95 loads and a true DOS session can be run from within Windows 95. The user is also able to reboot Windows 95 under DOS and Windows 95 can be run in real mode. Within these environments it is likely that current DOS viruses will run normally. No doubt Windows 95 will be updated, so only time will tell which viruses survive the new environment.

Some viruses do not load into memory. Instead, when the infected program is run, they infect another program.

Macro viruses

There are now macro viruses in existence, for example the Winword.Concept virus that infects Word 6 document files. This virus can infect Word 6 on any operating system including Windows 95. Many applications now have similar macro languages which could potentially be used to create viruses in the future.

Boot and partition sector viruses

The partition sector is the first part of a hard disk to be read after the system has started up. It contains information about the disk such as the number of sectors in each partition and the location of all the partitions. The partition sector is also called the Master Boot Record (MBR).

The boot sector is the part of every hard disk and diskette which is read by the computer when it starts up. The boot sector of a system disk contains the code necessary to load the system files; a data disk contains the code necessary to display the message that the PC cannot be booted from that disk.

Most PCs are set up to attempt to boot from the A: drive first. If the boot sector of a diskette is infected, the virus runs when you attempt to boot from the diskette, and infects the hard disk.

For example, if you leave a diskette in the drive overnight and then switch on your PC the next day, the following message, or similar, is displayed:

```
Non-system disk or disk error
Replace and press any key when ready
```

If the diskette is infected with a boot sector virus, that virus has already run, and your PC may already be infected.

Any Intel-based PC is vulnerable to boot and partition viruses. They can infect any PC, regardless of the operating system, since the virus runs before the system starts up.

The Windows 95 operating system is very different from DOS and in some cases more secure against infection. Changes in the boot sector structure, for example, are likely to cause your PC to fail to boot or hang, once infected by a boot sector virus. Once Windows 95 does boot, it may check the boot sector and might warn of any changes.

Companion viruses

If you have a COM file and an EXE file of the same name, DOS always runs the COM file in preference to the EXE file if no file extension is given. Companion viruses make use of this fact by creating COM files with the same name as the legitimate EXE files, thus ensuring they are executed. They then pass control to the original EXE file which runs normally. Companion viruses will run in a Windows 95 DOS session, and some may be effective under Windows 95.

A path companion virus creates an infected file with the same name as an executable file and places the infected file in a directory named earlier in the path. The infected file therefore runs in preference to the original file.

Overwriting viruses

An overwriting virus simply overwrites each file it infects with itself, so the program no longer functions. Since this is very easy to spot these viruses do not spread very well, and are not a real threat. Overwriting viruses will run in a Windows 95 DOS session.

Multipartite viruses

Some viruses use a combination of techniques to spread, and infect executable files, boot sectors and partition sectors. These will generally not be able to spread under Windows 95.

Droppers

A dropper is a program, not a virus itself, that installs a virus on the PC while performing another function. Droppers that attempt to spread boot sector viruses are unlikely to work under Windows 95.

The future

As Windows 95 becomes more widespread, it is likely that viruses will be written specifically for this operating system. Such viruses could be written as VxDs and be as capable as DOS viruses to infect and cause havoc.

1.3 Characteristics of viruses

Stealth

Although some virus infections are readily apparent to the user, the most successful viruses try to remain as inconspicuous as possible so that they can spread without being noticed. A virus which uses *stealth* is one that tries to conceal its presence on the disk so that everything appears to be running normally. Many boot sector viruses use a certain amount of stealth; after running they pass control to the original boot sector so that the PC starts up normally. A detailed discussion of stealth, and ways to counteract it, is given in the Virus Encyclopedia.

Windows 95 checks the boot sector as it starts up and will report any changes. Most stealth viruses copy the original boot sector and store it somewhere else on the hard disk. Problems occur when this copy is placed on an area used by Windows 95.

Polymorphism

Many virus detection programs work by looking for a known pattern of bytes in the code of the virus. A *polymorphic* virus is one that tries to avoid detection in this way by ensuring that its code does not have a fixed pattern of characters. Usually the virus achieves this by encrypting itself differently each time it runs.

The Toolkit can deal effectively with polymorphic viruses using the Generic Decryption Engine. This can decrypt the virus without knowing the encryption method, allowing virus-scanning software to identify the virus and repair the infected files. It achieves this extremely rapidly and without any time-wasting false alarms. The Generic Decryption Engine is built into the Toolkit's scanner, FindVirus.

More information on polymorphic viruses is given in the Virus Encyclopedia.

Virus names

Many viruses appear to have several different names. This happens because most viruses are named by the anti-virus researchers who identify them, rather than by their authors, who prefer to remain anonymous. Different researchers often give viruses different names, based on text within the virus code or where they were first discovered.

Dr Solomon's uses names which are approved by the Computer Anti-Virus Researchers Organisation (CARO). In addition, the Virus Encyclopedia lists any aliases by which the virus is commonly known.

Variants

Many viruses are found in a number of related variations, often because their authors have simply amended the code of existing viruses. The Virus Encyclopedia includes details of all known variants which the Toolkit is able to find and deal with.

How viruses spread

The most common way in which a virus is spread is via an infected diskette. Boot sector viruses are the most common type of virus, and they can only be transmitted by a diskette. People who use diskettes on a number of different PCs increase their chances of picking up an infected diskette and spreading the virus.

Some people mistakenly assume that shareware, free disks and games are the only sources of viruses. Although viruses are sometimes transmitted through these types of software, because they tend to be copied more, they have also been found in shrink-wrapped software distributed by major companies, and on diskettes accompanying hardware. For this reason, you should always scan all diskettes for viruses before they are used.

File viruses can also be spread by downloading infected programs from bulletin boards. You should take care to check any software transferred over a network or communications link before using it.

A workstation on a network can be infected in the same way as a standalone PC, and a virus can spread very quickly across a network. Since the effect of a virus infection can be particularly serious if a file server becomes infected, you should take particular care to protect networks from infection.

1.4 Other potential problems

When something goes wrong with a PC, it is easy to think it must be a virus. Unfortunately, there are many other problems which can disrupt work and destroy data. Some of these are described below.

Bugs

A bug is an unintentional fault in a program. Virtually all complex software contains bugs. Minor bugs merely cause inconvenience, while major bugs can cause catastrophic data loss. There is no way of detecting bugs, and the only defence is to ensure you back up your important data regularly.

Low-level software clashes

Low-level programs are those which work on disks directly. They are so-called because they function below the level of the operating system, which normally controls access to disks and enforces certain rules. Low-level programs include:

- Disk sector editors.
- Disk caching programs.
- Disk compression software.
- Defragmenters.

These tools are usually quite safe to use if you only run one at a time, but problems can occur if you run two or more low-level tools at the same time. If two or more tools try to access the disk, potentially dangerous clashes can result. As these tools become more common, this type of problem is more and more likely to occur.

To avoid problems with low-level tools:

- Always take a backup before using any disk utilities.
- Do not run more than one utility at the same time.
- Avoid using these tools at the same time as using memory-resident software.
- Always read the manuals and any README files supplied with the product. If the manufacturer has included any special warnings, there is usually a good reason for them!

Trojans

Trojans are programs which do something unexpected and usually damaging. They are less widespread than viruses because they do not replicate, but they can represent a threat when copied. Many people confuse the two - the AIDS Information Diskette, often cited by the media as an example of a virus, was actually a trojan. Also, viruses sometimes contain trojans.

You are unlikely to encounter a trojan if you always obtain your software from reputable sources, but the main defence against damage by such programs is to back up your system.

The Toolkit finds and identifies some known trojans and treats them in the same way as viruses.

Time bombs and logic bombs

These are particular types of trojan. A time bomb is set off on a particular date, while a logic bomb is triggered by a specific set of conditions, such as the number of files on a disk or a certain sequence of characters being entered. Both types usually do something damaging.

Jokes

Some programs claim to be doing something destructive to your computer, but are actually harmless jokes. For example, a message may appear suggesting that your hard disk is about to be reformatted. Unfortunately, it is easy to over-react to the joke and cause more damage by trying to eradicate something that is not, in fact, a virus.

The Toolkit finds and identifies a number of widespread joke programs.

Human Error

When something goes wrong with your PC, or you lose data, the most likely cause is not a virus or a software problem, but human error. Everybody makes mistakes such as pressing the wrong key sequence or typing DEL *.* in the wrong folder, and these can have drastic results.

Remember that the most valuable part of your computer is the data you have stored on it. Hardware and programs can be replaced but you can only replace your data if you have backed it up.

1.5 What you can do

The data recovery specialists at Dr Solomon's see a lot of people who have lost their data. Fortunately, the data can nearly always be restored and we can usually identify the reason that it was lost in the first place.

Although viruses are a problem, the scale of the problem should be kept in perspective. The most common reason for losing data is human error. The second most common cause is hardware failure, followed by software problems and bugs. Viruses come a poor fourth.

However, implementing a straightforward anti-virus policy will help protect your data from all kinds of loss, including viruses. In particular, you should consider the following three elements of protection:

- Prevention - to limit the spread of viruses.
- Detection - to ensure that if a virus does get through the defences, it is discovered as quickly as possible.
- Recovery - to ensure that if any files are lost or damaged, they can be restored as quickly as possible.

Using the Anti-Virus Toolkit is obviously a significant part of the detection and recovery policy, but some other elements of a sensible anti-virus policy are suggested below.

Backups

The most important precaution you can take against any kind of data loss is to make regular backups of your system. If you do not back up your data regularly, it is at risk.

Remember to check your backups frequently and make sure that you can restore your data from them.

Check that you have clean copies of all your executable files on diskette. All your backup diskettes and your boot diskettes should be write-protected.

Software sources

Make sure that all your software comes from a reputable source. Check that software is in its original packaging.

Never use pirated software. Even if you feel entitled to use another copy temporarily (for example, because you left your licensed copy at another site) remember that the copy may expose you to virus infection.

Software can enter your PC via the communications ports as well as via portable media. Take care when transferring software to and from laptops and across networks and when downloading files from bulletin boards.

Diskettes and other media

The risk of virus infection via diskette is particularly high, but you can take some simple steps to increase security.

- Keep diskettes write-protected wherever possible, to prevent viruses being copied.
- Do not leave diskettes in the drive when you turn off the PC. This will prevent you accidentally trying to boot from a diskette infected with a boot sector virus.
- If you do accidentally boot from a non-bootable diskette, switch off and start again instead of proceeding with the boot from the C: drive.
- Change the CMOS setting of your PC so it boots from the C: drive first rather than the A: drive. (This is not always possible on SCSI drives).
- Use alternative methods of file transfer where possible.
- Remember that files on tape may have been infected when the back-up was made.

Employee co-operation

You need the willing co-operation of your employees in any anti-virus policy. If members of staff think that they are likely to be disciplined if they discover a virus, they are unlikely to report any problems.

Some companies have attempted to ban the playing of games. It is much a better policy to ensure that games come from a reputable source and are checked before use. It can be useful to give one person or a small group the responsibility of checking and distributing games software.

1.6 The Anti-Virus Toolkit

The Anti-Virus Toolkit for Windows 95 provides a set of tools for the detection and removal of viruses. There are two major types of anti-virus software.

- A *scanner* is a program that searches for viruses. Since new viruses are always appearing, scanners need to be updated regularly.
- A *checksummer* detects changes in files. It calculates a unique numeric fingerprint, known as a checksum, for each file to be protected. The checksummer can then be run to re-calculate this fingerprint to monitor any differences. Executable files do not usually change, so if there is a difference in the fingerprint, a virus may be present.

Dr. Solomon's Anti-Virus Toolkit for Windows 95 includes scanners and a checksummer, which operate as described below.

FindVirus

FindVirus is a scanner which you can use regularly to scan your hard disks and any incoming diskettes. It will find and report any known virus, that is, one held in the current version of the driver file. It also includes an optional heuristic scanner which looks inside files for suspicious code that may indicate a previously unknown virus.

FindVirus will find viruses in files, boot sectors and partition sectors. It can also be used to repair virus infections. FindVirus can be used to scan incoming diskettes and files on a sheep-dip PC - one that is always used for that purpose. FindVirus scans very quickly and can be used for scanning hard disks on a daily basis.

VirusGuard

VirusGuard is a memory-resident scanner which scans continuously for viruses. It identifies known viruses and prevents access to any file if a virus is found. VirusGuard detects virtually all the viruses in the current driver file. However there are a few particularly complex polymorphic viruses which VirusGuard can detect but cannot prevent from running.

WinGuard

WinGuard is a Windows memory-resident scanner (VxD) which takes over from VirusGuard when Windows in run. When both VirusGuard and WinGuard are enabled (as recommended), then control is passed automatically between them as Windows is started up or shut down.

Using Windows technology, WinGuard is able to detect all known viruses, including complex polymorphic, quickly and accurately.

ViVerify

ViVerify is a checksummer which detects changes in executable files that may have been caused by a virus infection. Initially you can use ViVerify to calculate a fingerprint, or checksum, for each file. You can then run ViVerify regularly to re-calculate this fingerprint and check if there are any changes. Although a change to an executable file does not necessarily mean that the file is infected, executable code does not normally change. ViVerify reports any possible virus, even a previously undiscovered one.

The Virus Encyclopedia

The on-line Virus Encyclopedia includes details of the most common viruses which the Toolkit can detect, including any variants. The on-line Virus Encyclopedia is more comprehensive than the Encyclopedia manual.

This page has been left blank

2. Installing the Toolkit

This chapter explains how to install the Anti-Virus Toolkit for Windows 95 on your PC.

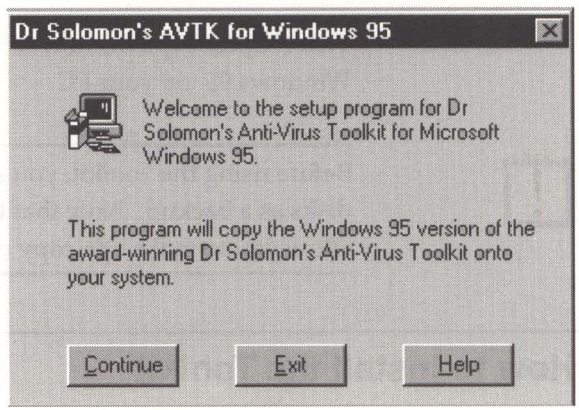
Before using the Toolkit, you should make a copy of the program disks as a backup. Note that the terms of your licence agreement allow you to make one copy only.

2.1 How to install the Toolkit

By following the instructions below, you first check that your PC is clean (virus-free). You then install the Toolkit to ensure it remains clean.

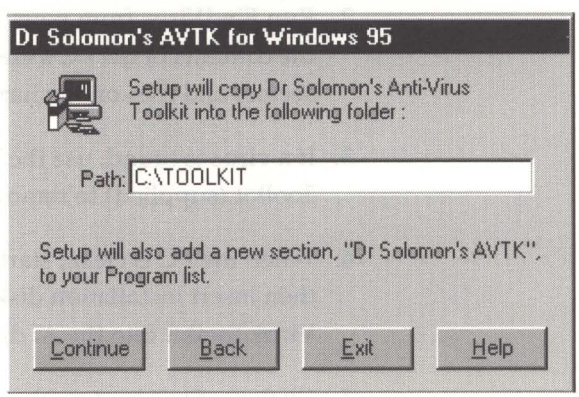
1. Boot from a clean, write-protected, DOS system diskette.
2. Run FindVirus from your Toolkit DOS diskette. This checks the contents of the PC's memory and the boot sectors, partition sectors and files on the hard disk.
3. If a virus is found, use the DOS version of the Anti-Virus Toolkit (supplied) to remove the infection.
4. When the PC is clean, start up Windows 95 in the usual way, then insert installation diskette 1 of the Windows 95 Anti-Virus Toolkit into the A: drive.
5. Click the Start button, then click Run. In the Open box, type `A:\SETUP` and press ↵.

6. You are prompted to confirm that you wish to install the Windows 95 version of the Anti-Virus Toolkit.


Dr Solomon's AVTK for Windows 95
Welcome to the setup program for Dr Solomon's Anti-Virus Toolkit for Microsoft Windows 95.
This program will copy the Windows 95 version of the award-winning Dr Solomon's Anti-Virus Toolkit onto your system.
Continue
Exit
Help

Press ↵ to continue with the installation.

7. The Toolkit is installed on drive C in a folder called TOOLKIT unless you specify otherwise:


Dr Solomon's AVTK for Windows 95
Setup will copy Dr Solomon's Anti-Virus Toolkit into the following folder:
Path: C:\TOOLKIT
Setup will also add a new section, "Dr Solomon's AVTK", to your Program list.
Continue
Back
Exit
Help

8. Specify an alternative path if you want to and press ↵.

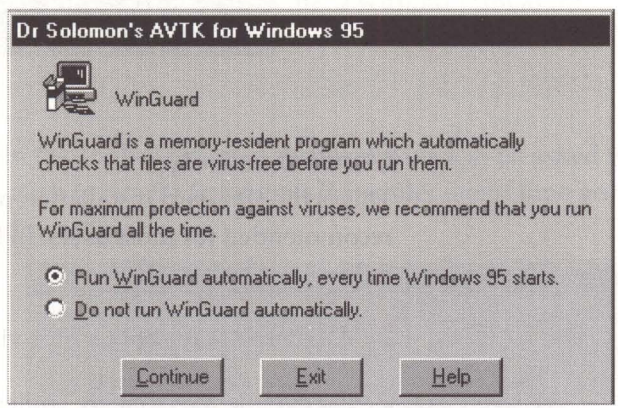
9. The installation process then starts.

You are prompted to insert further disks during the installation process. You can cancel the installation at any time by pressing Esc. If you then want to re-install, you should first delete

any files in the Toolkit folder that were created in the original installation.

WinGuard

WinGuard is a memory-resident program which runs under Windows 95. It checks that files and disks are free from infection before permitting access to them. You are prompted to specify whether you want WinGuard to run automatically each time Windows 95 starts. You are strongly recommended to enable both WinGuard and VirusGuard (described below).


Dr Solomon's AVTK for Windows 95
WinGuard
WinGuard is a memory-resident program which automatically checks that files are virus-free before you run them.
For maximum protection against viruses, we recommend that you run WinGuard all the time.
Run WinGuard automatically, every time Windows 95 starts.
Do not run WinGuard automatically.
Continue
Exit
Help

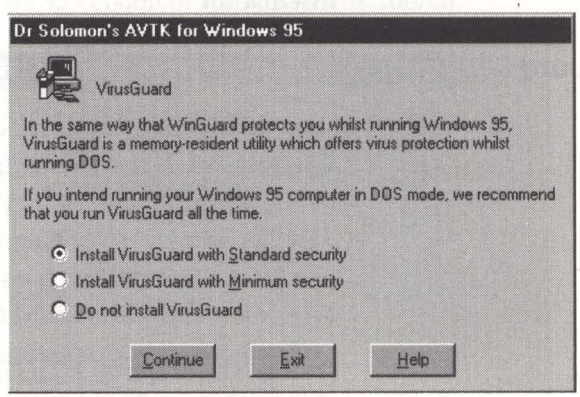
Make sure the option you require is selected then press ↵.

The install process copies files from the diskettes and adds necessary lines to Windows system files. On-screen help is available if you need more information, and further details are also given in Chapter 4 "Guarding against Viruses" in this manual.

VirusGuard

VirusGuard is a memory-resident program which runs under DOS. It checks that files and disks are free from infection before permitting access to them. You can choose between installing it with standard security, installing it with minimum security or not installing the program. You are strongly recommended to enable both VirusGuard and WinGuard (described above).

You can choose to run VirusGuard in one of two security levels.


Dr Solomon's AVTK for Windows 95
VirusGuard
In the same way that WinGuard protects you whilst running Windows 95, VirusGuard is a memory-resident utility which offers virus protection whilst running DOS.
If you intend running your Windows 95 computer in DOS mode, we recommend that you run VirusGuard all the time.
Install VirusGuard with Standard security
Install VirusGuard with Minimum security
Do not install VirusGuard
Continue
Exit
Help

Standard security

This is the standard installation mode, and the one that is recommended for most users. In this mode, VirusGuard scans the following:

- All diskettes for boot sector viruses.
- Executable files that are copied.
- Executable files when they are run.

Minimum security

With this option set, VirusGuard only scans the following:

- All diskettes for boot sector viruses.
- Executable files copied from diskette.
- Executable files when they are run.

In all cases, when scanning executable files, VirusGuard looks for files with the following extensions:

APP	EXE	SYS
BIN	OVL	XTP
COM	OVR	
DLL	SCR	

You can also optionally check files with the FON extension (see "Changing the pop-up message" on Page 104).

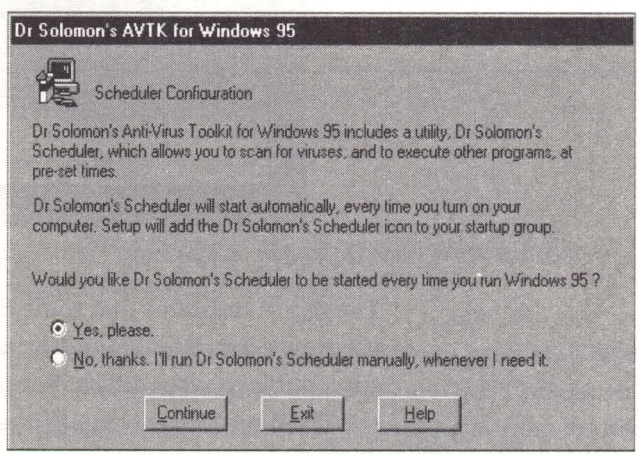
If you are unsure of the security level to choose, select the default setting of standard security. You can change it later if you wish (see "Changing the security level" on Page 105).

Use the ↓ and ↑ keys to select the option you want, then press ↵.

You should NOT use VirusGuard without WinGuard.

Installing the Scheduler

When the Toolkit has been installed, you will be asked whether you wish to run Dr Solomon's Scheduler every time you use Windows 95.


Dr Solomon's AVTK for Windows 95
Scheduler Configuration
Dr Solomon's Anti-Virus Toolkit for Windows 95 includes a utility, Dr Solomon's Scheduler, which allows you to scan for viruses, and to execute other programs, at pre-set times.
Dr Solomon's Scheduler will start automatically, every time you turn on your computer. Setup will add the Dr Solomon's Scheduler icon to your startup group.
Would you like Dr Solomon's Scheduler to be started every time you run Windows 95 ?
Yes, please.
No, thanks. I'll run Dr Solomon's Scheduler manually, whenever I need it.
Continue
Exit
Help

This memory-resident tool allows you to run virus checks and other programs at pre-set times. If you select Yes, an icon is added to your Windows Start menu, and the Scheduler will be started whenever you log on.

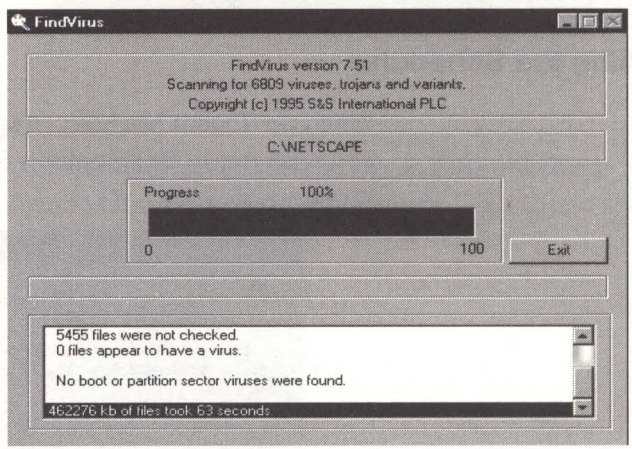
If you select No, the icon is not added to the Start menu. In this case, you run Dr Solomon's Scheduler by clicking on its name in the Dr. Solomon's Anti-Virus Toolkit menu.

The Scheduler is described in detail in Chapter 7, "Using the Scheduler".

Completion of installation

When the installation process is complete, a window shows you what Anti-Virus Toolkit features are now available on your computer. Close the window to proceed.

FindVirus now runs automatically to scan your local hard disks for any viruses. If your PC is free from viruses, a screen of the following format is displayed:



The report indicates that some files have not been checked. This is because, by default, FindVirus only checks files that are most susceptible to virus attack. For more information on FindVirus, see "Finding Viruses - FindVirus" on Page 39.

If the screen reports a virus on your PC, do not panic! See Chapter 6, "Virus Repair and Removal", for information about what to do.

The installation is now complete, and your PC has been scanned for viruses. Press ↵ to close the FindVirus window.

You are told that Setup is complete, and reminded to register. Press ↵ to return to the main Windows 95 screen.

Note that you must restart the PC before the memory-resident guard programs VirusGuard and WinGuard become effective.

If you have problems installing the Toolkit, check that you have followed the procedure in this manual. If you cannot resolve the problem, contact Dr Solomon's Technical Support. See "If you need help" on Page xiv.

2.2 README files

As part of the installation, a file called README95.TXT is copied to the Toolkit folder. If you install the DOS Toolkit a file called README.TXT is also copied to the Toolkit folder. These files contain amendments to the manuals, and provide information on the latest Toolkit developments, so you are recommended to read them carefully.

These text files can be accessed by any of the normal methods.

2.3 How to uninstall the Toolkit

To uninstall the Toolkit:

1. Make sure WinGuard is disabled; see "WinGuard Configuration dialog" on Page 34.
2. Make sure that Dr Solomon's Scheduler is not in the StartUp folder. If it is, then remove it and restart the PC. Refer to the information on the Windows 95 operating system for the removal procedure.
3. Start the application 'uninstal' which is in the Toolkit directory.
4. Confirm that you want to remove the Toolkit when you see the prompt.
5. When prompted, specify the Toolkit directory; enter its full path.

6. If you see the message 'Cannot delete C:\.....\tk_schen.exe' go back and complete Step 2.

7. Respond to the prompt to move or delete any data files containing custom setup information.

2.4 Upgrading the Toolkit

The Toolkit is updated monthly to deal with new viruses. Dr Solomon's recommends that you maintain a subscription to the upgrade service to ensure complete protection from viruses. See "Registration and upgrades" on Page xiii.

Upgrades are available on a quarterly or monthly basis, and consist of a complete set of disks. To install the upgrade:

1. Insert installation diskette 1 into the A: drive.

2. Click the Start button, then click Run...

3. In the Open box, type `A:\SETUP` and press ↵. Follow the instructions displayed on the screen.

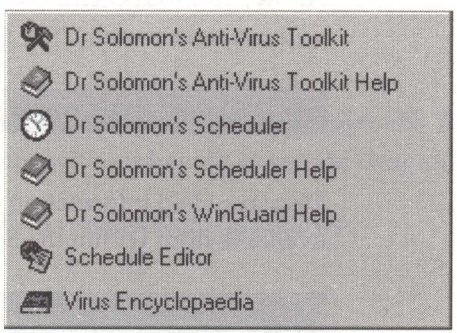
3. Finding your Way Around

This chapter explains how to start up and use the Toolkit. It explains the options available from the menus and explains how to move around the user interface.

3.1 Starting the Toolkit

When the Windows installation is complete, the Anti-Virus Toolkit appears in the list of programs you may run from the Windows 95 desktop.

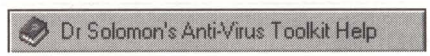
Click on Start, point to the Programs option then point to Dr Solomon's AVTK. The following menu is displayed:



You can of course move the Toolkit options to another menu if you wish. See your Windows documentation for details.

The menu options are as follows:

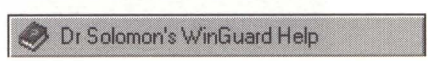
Starts the Toolkit and displays the main screen.



Displays help information for the Windows 95 Toolkit. This is also available from within the Toolkit.

Allows you to run virus scans, or other programs, at set times without intervention. See Chapter 7, "Using the Scheduler".

Displays Help information for using the Scheduler. This is also available from within the Schedule Editor

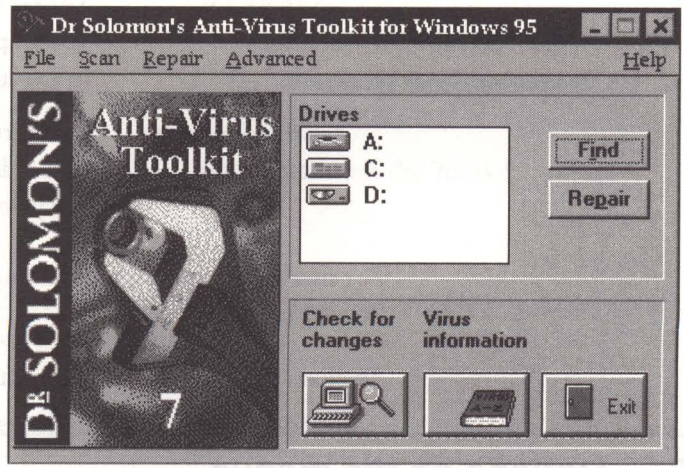


Displays Help information for using the WinGuard program.

Enables you to set up scheduled events. See Chapter 7, "Using the Scheduler".

Displays the Virus Encyclopedia directly, enabling you to search for details of a particular virus.

To start up the Toolkit, click on the Toolkit icon. The following window is displayed:



3.2 The main screen

The main screen provides quick access to the Toolkit's most useful items without having to use the drop-down menus.

The short cuts available are as follows:

Process	Short Cut
To scan for viruses	Select one or more disk drives from the displayed list, then choose Find to scan for any known virus using FindVirus.
To repair infected files and diskette boot sectors	Select a disk drive from the displayed list, then choose Repair to detect viruses and repair files and diskette boot sectors.

Process	Short Cut
To check for changes	The Check for Changes option allows you to perform a check for any changes in executable files, using ViVerify.
Displaying virus information	The Virus Information option allows you to browse through the Virus Encyclopaedia to find information.

For more information on running these options, see Chapter 5, "Checking for Viruses".

To close the Toolkit, select Exit from the File menu or press Esc.

3.3 Options on the menus

Apart from the short cuts on the main screen, you can select the Toolkit features from a number of drop-down menus. These are described below.

File menu

The File menu includes options for managing files.

Menu Option	Function
Load Configuration	Allows you to load a previously-saved file containing particular Toolkit settings. See Chapter 11, "Toolkit Configuration" for more details.
Save Configuration	Allows you to save the current Toolkit settings so that they can be used later. See Chapter 11, "Toolkit Configuration" for more details.

Menu Option	Function
Shred	Deletes a file in a way that ensures it cannot be recovered. See "Shredding files" on page 67 for more details.
Exit	Exits from the Toolkit.

Scan menu

The Scan menu includes options which enable you to set up and run the virus-checking tools.

Menu Option	Function
Find viruses	Runs FindVirus, which scans for viruses on any hard disk or diskette.
Check for Changes	Runs ViVerify, which can tell if an executable file has been altered.
Check memory	Scans both conventional and high memory for any memory-resident viruses.

Repair menu

The Repair menu includes options which allow you to repair infected files and diskettes.

Menu Option	Function
Repair Drive	Repairs any infected files on the specified drive.
Replace Boot Sector	Replaces a corrupted boot sector on a diskette with a clean copy.

For more details of these options, see Chapter 6, "Virus Repair and Removal".

Advanced menu

The Advanced menu includes additional options.

Menu Option	Function
Inspect disk	Allows you to examine a diskette or hard disk at a low level.
Inspect file	Allows you to examine the contents of a file in ASCII or hexadecimal.
Virus Encyclopaedia	Allows you to view the on-line Virus Encyclopaedia and to search for particular information.
Schedule	Allows you to set up schedules to perform events at particular times. See Chapter 7, "Using the Scheduler" for more details.

Help menu

The Help menu includes the following options.

Menu Option	Function
Index	Displays an alphabetic list of help topics available. You can scroll through the list or search for a particular topic.
Using help	Explains how to find your way through the help system.
Keyboard	Explains how to choose options and make selections using the keyboard.
Procedures	Displays a reminder of what to do if you find a virus.
Virus-L FAQ	Answers a number of frequently-asked questions about viruses.

4. Guarding against Viruses

Although you may run your PC under Windows 95 for most of the time, it is still vulnerable to DOS viruses as well as Windows viruses. The PC runs under DOS briefly each time it is started up, and it is possible to shut down Windows 95 in such a way that the PC remains running under DOS alone.

Two memory resident programs are available, both of which scan for viruses whenever files or disks are accessed. If you have installed both programs, as recommended, then one or other of them will be loaded in your computer's memory at all times. These programs detect any signs of a virus infection at the earliest possible opportunity. The two programs are:

- WinGuard, a Windows memory-resident scanner (VxD) which takes over from VirusGuard when Windows in run. When both VirusGuard and WinGuard are enabled (as recommended), then control is passed automatically between them as Windows is started up or shut down. Using Windows technology, WinGuard is able to quickly and accurately detect all known viruses, including complex polymorphic ones.

- VirusGuard, a DOS memory-resident scanner which scans for viruses whenever an executable file is accessed. It identifies known viruses and prevents access to any file if a virus is found. VirusGuard detects virtually all the viruses in the current driver file. However there are a few particularly complex polymorphic viruses which VirusGuard can detect in memory but cannot prevent from running.

We recommend that you enable both VirusGuard and WinGuard during installation. Using these two scanners, you are fully protected under both DOS and Windows.

4.1 Using WinGuard

WinGuard is automatically started when Windows is run and will operate normally without user intervention. The WinGuard status information is displayed momentarily and then minimized to the task bar.

If WinGuard is unable to be loaded, Windows 95 will not load either. Instead, a message is displayed. Follow the virus checking instructions in Chapter 5, *Checking for Viruses*.

If a virus is found

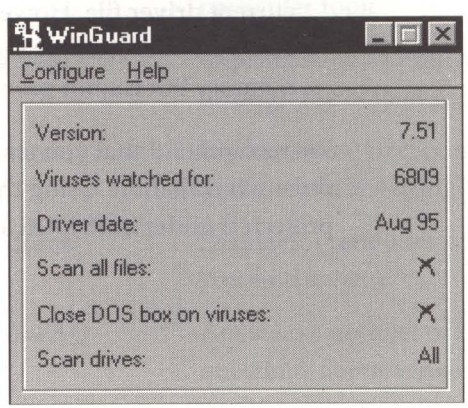
If a virus is detected, access to the file is prevented. In addition, an alarm sounds and a dialog is displayed in front of any program you are running.

In addition, your application may warn you of a problem. The message and the exact sequence of events will depend on the particular application you are running at the time.

Follow the instructions in Chapter 5, *Checking for Viruses*, to run FindVirus on the infected disk and repair the file(s).

Configuring WinGuard

The WinGuard interface is used to change the configuration. Simply double-click on WinGuard in the task bar to open the dialog. The current settings are shown.

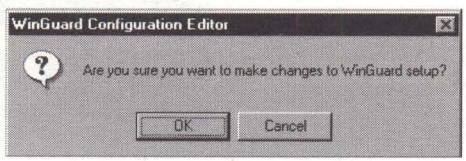


The Configure menu provides two options:

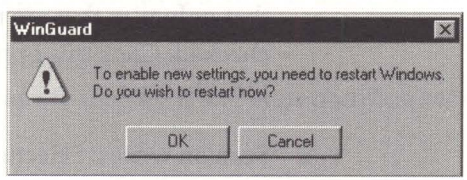
- The WinGuard option allows you to change the settings that govern how WinGuard operates.
- The Front End option defines the messages that will be displayed under different situations when a virus is found.

Full on-line Help is provided from the Help menu and Help is available from within the dialogs.

When you change some settings in either of these dialogs, you see the following prompt:



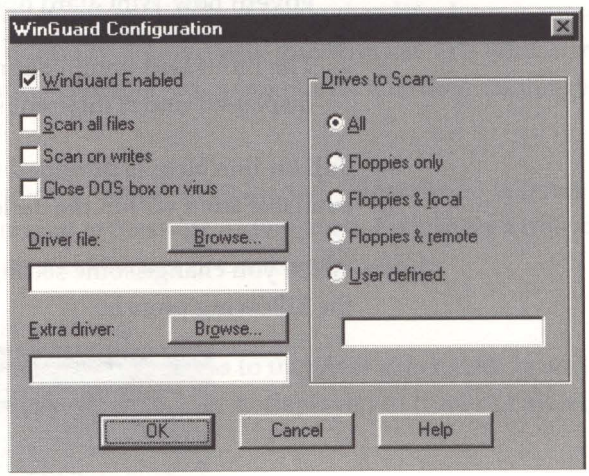
After you click on OK, you are prompted to restart Windows so that the new configuration can come into effect.



If you click on OK, Windows is restarted automatically. If you do not want Windows restarted at this point, click on Cancel. The new configuration is effective only when Windows restarts.

WinGuard Configuration dialog

The WinGuard Configuration dialog contains a number of settings:

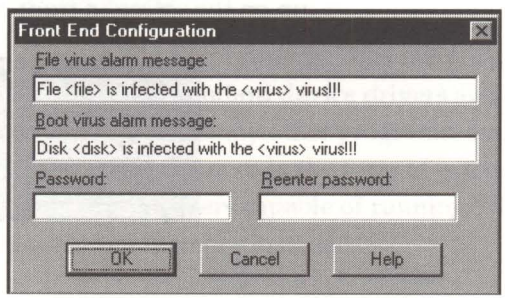


- WinGuard Enabled: This option turns WinGuard on and off.
- Scan all files: The default setting has this option unselected, so that only files that are most susceptible to virus attack are checked. Click this option so that it is selected if you want *all* files checked.
- Scan on writes: Selecting this option ensures that files are scanned as they are written to your local hard disk, such as downloading from the Internet, file decompressions, etc. This option slows down the process.
- Close DOS box on Viruses: With this option selected, if a virus is found, the DOS session is closed.
- Drives to scan: Click on one of the options. If you select "User defined" type in the drive letters in the text field. More than one drive can be specified (no colons or spaces are required). Only files from the specified drive(s) will be checked by WinGuard.

Front End Configuration dialog

This dialog allows you to change the messages displayed when a virus is detected. The words in angle brackets, <>, will be replaced with the appropriate name(s), when the messages are displayed.

There are four text fields into which you can type a message. You can also enter a configuration password.



- File virus alarm message
  The message to display if a virus is found in a file.

- Boot virus alarm message
  The message to display if a boot or partition sector virus is found.

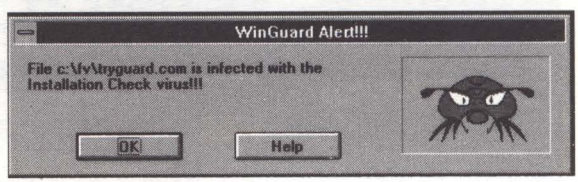
- Password/Reenter Password
  By entering a password in these fields, only users who know the password will be able to update the WinGuard configuration. Whenever *either* option is selected from the WinGuard Configuration menu, the user will be prompted for the password. Neither the WinGuard Configuration or the Front End Configuration dialog will be displayed until the password is entered correctly.

Advanced features of WinGuard

A utility program called WTKUTIL allows you to examine and/or change certain WinGuard settings. The options offered by this program are described in "" on page 127.

If WinGuard reports a virus

If WinGuard detects a virus, an alarm sounds and a warning pops up on the screen in front of any program you are running.



The pop-up tells you what has caused the WinGuard alarm and which file or disk has caused the problem.

You will not be able to copy or run the infected file.

If the alarm is sounded and displayed, follow these steps:

1. Read the message in the pop-up and then press the Ctrl key, or select OK.
2. Exit in the normal way from whatever you were doing and save any files you were working on.
3. Shut down Windows 95.
4. Power off and boot the PC from a clean, write-protected, DOS system diskette.
5. Run DOS FindVirus from the original DOS Toolkit diskette to scan the appropriate disk.

Chapter 6 gives details of how to remove a virus and repair files.

4.2 Using VirusGuard

If you specified, during installation, that VirusGuard should run automatically, then it runs each time the computer is started up. It is disabled as Windows is started and re-enabled if you exit to DOS, and normally operates without user intervention.

How VirusGuard uses memory under DOS

Most PCs have up to 640 Kb of conventional memory, which is used to run DOS and the standard device drivers and commands. However, VirusGuard, like many other programs, works faster if your PC has additional resources in the form of extended or expanded memory. Computers capable of running Windows 95 already have extended memory installed.

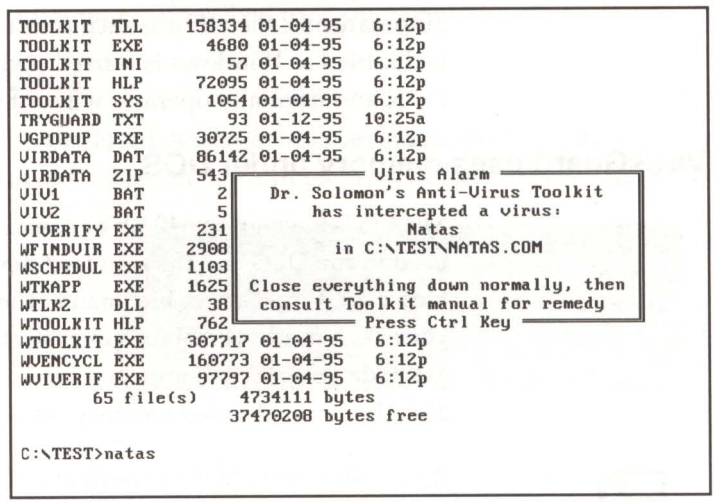
If you are unsure of the type or amount of memory your PC has, you can find out by typing the DOS command MEM at the system prompt.

If you have expanded or extended memory, VirusGuard automatically uses the most appropriate memory option when it runs. It checks for extended memory first, and if this is not present, or if there is not enough contiguous extended memory available, it looks for expanded memory.

If necessary, VirusGuard can make use of a RAM drive, or even access the virus driver file from the hard disk (provided that the GUARD.COM and DRV files are copied there and run from there). These measures degrade performance and should not be necessary on any PC that can run Windows 95.

If VirusGuard reports a virus

If VirusGuard detects a virus, an alarm sounds and a warning pops up on the screen in front of any program you are running.



The pop-up tells you what has caused the VirusGuard alarm and which file or disk has caused the problem.

You will not be able to copy or run the infected file.

If the alarm is sounded and displayed, follow these steps:

1. Read the message in the pop-up and then press the Ctrl key, or select OK.
2. Exit in the normal way from whatever you were doing and save any files you were working on.
3. Return to the system prompt.
4. Power off and boot the PC from a clean, write-protected, DOS system diskette.
5. Run DOS FindVirus from the original DOS Toolkit diskette to scan the appropriate disk.

Chapter 6 gives details of how to remove a virus and repair files.

5. Checking for Viruses

This chapter provides a step-by-step explanation of running FindVirus, ViVerify, Inspect File and Inspect Disk from the user interface. For details of how to run the programs from the command line or in batch files, see Chapter 8, "Advanced Virus Detection" and Chapter 10, "Advanced Virus Checking".

5.1 Finding Viruses - FindVirus

FindVirus scans for all the boot sector, partition sector and file viruses listed in the virus driver file. You can use FindVirus to ensure that any hard disk or diskette is free from all known viruses.

An option also allows you to run a heuristic scanner. This technique looks inside files for suspect code combinations that may be a result of new viruses not yet included in the virus driver file.

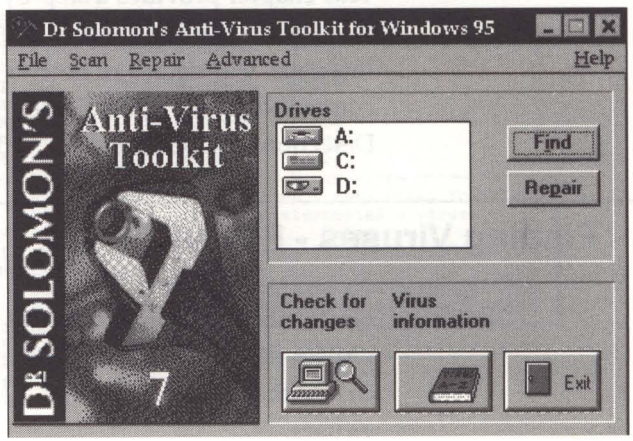
When to use FindVirus

You should use FindVirus to scan all incoming diskettes and files to ensure they are free from viruses.

You can also use FindVirus to help clean up after a virus outbreak. It will tell you which files are infected, and with what virus. It can also be used to repair the infected files and diskette boot sector viruses.

Running FindVirus from the main screen

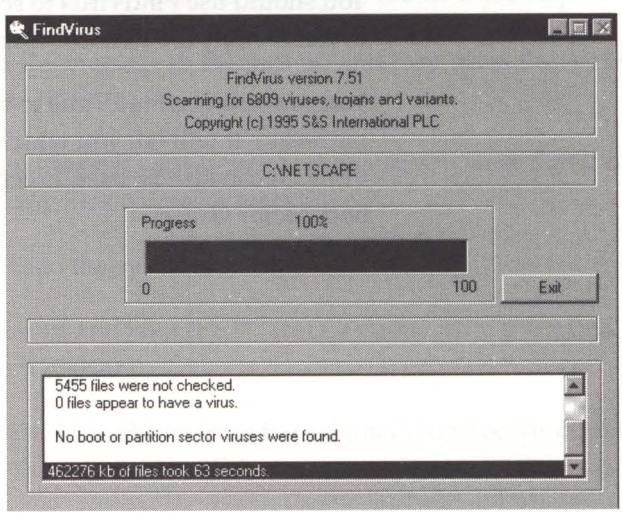
You can run FindVirus from the Toolkit main screen:



Follow these steps:

1. In the Drives box, select the drive(s) you want to check.

2. Select Find. The selected drives are scanned for viruses. When each scan is complete, a report of the following format is displayed:



3. If you have selected a diskette drive, when the scan is complete you will be asked if you want to scan another diskette. If so, insert the next diskette before choosing Yes.

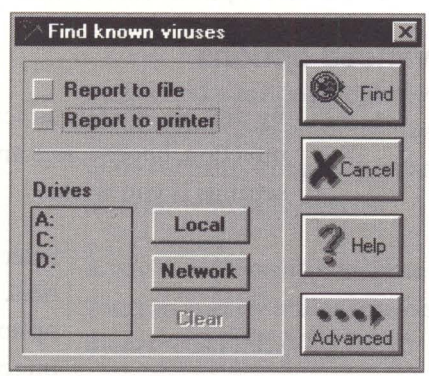
4. If your disk is free from viruses, the message *All clear* is displayed.

If a virus is found, do not panic! See Chapter 6, "Virus Repair and Removal", for information about what to do.

Running FindVirus from the main screen uses the default settings. If you want to change any of these, you should run FindVirus from the Scan drop-down menu as described in the next section.

Running FindVirus from the Scan menu

1. Select Find Viruses from the Scan menu. The following dialog box is displayed:



2. The settings and options are as follows:

Report to — By default, a report of the scan is displayed on the screen. In addition, you can choose to direct the report to a file, to a printer, or to both.

If you choose Report to file, the report will be saved in a file called FINDVIRU.REP in the TOOLKIT folder. You can change this filename using a setting on the Advanced dialog box.

If you choose Report to printer, the report will be sent to your default system printer. Make sure it is connected, loaded with paper and on-line.

Drives — Select the drives you want to scan. Choose Local to scan all the hard drives on your PC. Select Network to scan all network drives. Select Clear to clear any selections you have made.

3. These settings are suitable in most cases. You can start the scanning process by selecting Find or pressing ↵. Additional options are available by selecting the Advanced dialog box.

FindVirus advanced options

By default, FindVirus scans files most susceptible to virus infection, boot sectors and partition sectors. You can change these settings if you wish.

Select Data files to scan all non-executable files. Normally, you need only select this option if you are cleaning up after a virus infection.

Select ZIP, ARJ to scan files which have been archived using PKARC, PKZIP, LHA or ARJ.

Select PKLite if you want FindVirus to scan files compressed using PKLite, LZExe ICE, DIET or CRYPTCOM.

You should only deselect Boot sectors if this causes a particular problem, for example if you are scanning a network drive that doesn't have a boot sector.

Folder — If you only want to scan a particular folder, enter its path here. FindVirus then only scans files in the named folder and those below it. You should only use this option if you are absolutely sure that the virus is in a particular location. It is always much safer to scan the entire drive.

Other options — Select Beep on each virus if you need this extra warning when a virus is found.

Choose Multiple floppy disks if you want to scan more than one diskette in the same drive. You are prompted to insert the next diskette when each one has to be scanned.

Choose Heuristic scanner if you want to run extra checks for potential new viruses. This offers extra protection for users who need more security, but can increase scanning times by approximately 50%.

Report — If you want to send the virus report to a file, you can specify a filename here. The default filename is FINDVIRU.REP.

Additional options — This shows the command line for the options you have chosen. You can modify this directly if you wish. A full description of the various switches is given in Chapter 8, "Advanced Virus Detection".

When you have set any additional advanced options, select Back to return to the main FindVirus dialog box. Then select Scan to start the scan.

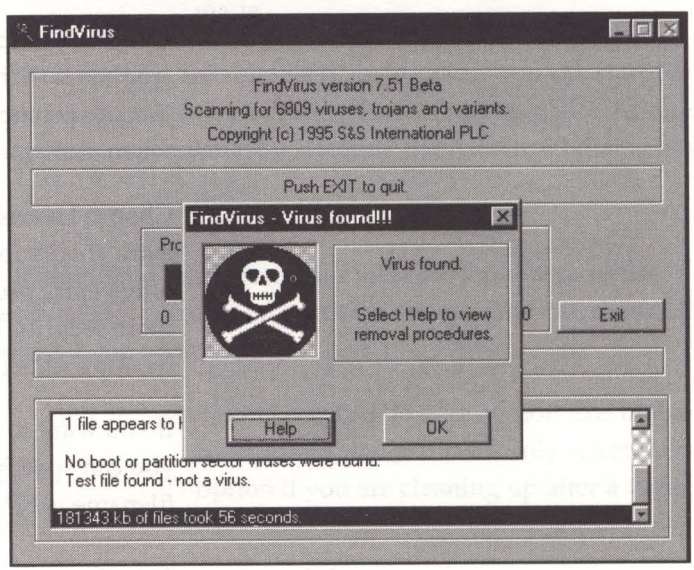
If your disk is free from viruses, the message *All clear* is displayed.

If a virus is found, do not panic! See Chapter 6, "Virus Repair and Removal", for information about what to do.

You can save the changed FindVirus settings for future use. Select Save Configuration from the File menu. For more information, see Chapter 11, "Toolkit Configuration".

If FindVirus reports a virus

Whenever you run FindVirus, it displays a screen of information. If a virus is found, it sounds an alarm and displays details of the virus in the following format:


FindVirus
FindVirus version 7.51 Beta
Scanning for 6809 viruses, trojans and variants.
Copyright (c) 1995 S&S International PLC
Push EXIT to quit
FindVirus - Virus found!!!
Virus found.
Select Help to view removal procedures.
Exit
Help
OK
No boot or partition sector viruses were found.
Test file found - not a virus.
181343 kb of files took 56 seconds

Read the message and make a note of the virus found. Exit in the normal way from whatever you were doing and save any files you were working on.

For details of how to repair the virus infection, see Chapter 6, "Virus Repair and Removal".

5.2 Inspecting disks and files

If you click on Advanced in the Toolkit menu bar, the following options are displayed:

Menu Option	Function
Inspect disk	Allows you to examine a diskette or hard disk at a low level.
Inspect file	Allows you to examine the contents of a file in ASCII or hexadecimal.
Virus encyclopaedia	Allows you to view the on-line Virus Encyclopaedia and to search for particular information.
Schedule	Allows you to set FindVirus and ViVerify to run at a particular time.

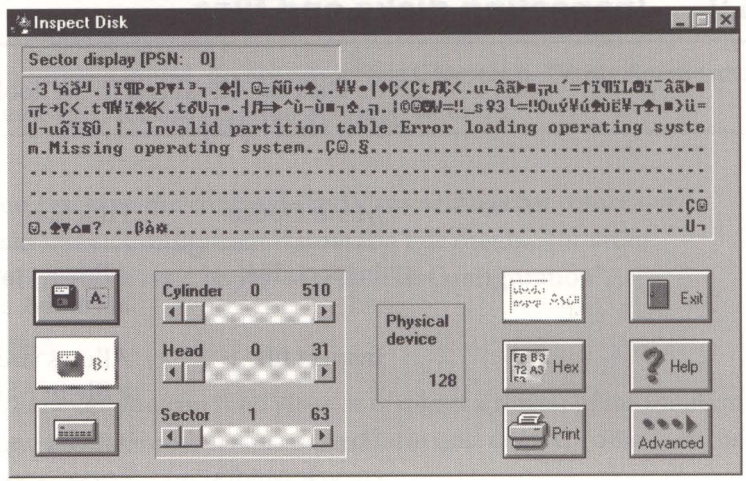
Inspect disk

Inspect disk enables you to examine hard disks and diskettes at a low level. It is safe to use because no data is written to the disk. To make the best use of Inspect Disk you need to be familiar with the content and structure of disks.

Inspect Disk allows you to examine the boot sectors of diskettes and the partition and boot sectors of hard disks. Suspect code in these areas may indicate a virus infection.

To examine a disk, select Inspect disk from the Advanced menu.

A screen of the following format is displayed:



Select the drive you want to check from the buttons on the left. Inspect Disk detects which disk drives are installed, and you can select the appropriate drive from those displayed.

If you have only one physical hard drive, it will be shown as a single drive even if it is divided into a number of logical drives. Drives A: and B: refer to physical devices 0 and 1.

If you have more than one physical hard disk, you can select only the first drive from this screen. Use the Advanced option screen to choose other hard disks.

You can navigate around the disk using the Cylinder, Head and Sector scrollbars. The numbers at the right of each scrollbar indicate the maximum values allowed.

On a hard disk, the partition sector is usually at cylinder 0, head 0, sector 1, and the DOS boot sector is usually at cylinder 0, head 1, sector 1. On a diskette, the boot sector is usually at cylinder 0, head 0, sector 1.

You can choose between displaying the disk contents as ASCII or as hexadecimal.

If you select Print, the contents of the current sector are printed on the default system printer.

If you want to look at a different diskette, simply swap it and press Space. The currently selected sector on the new diskette is displayed.

You can override the standard settings by means of the Advanced option menu:

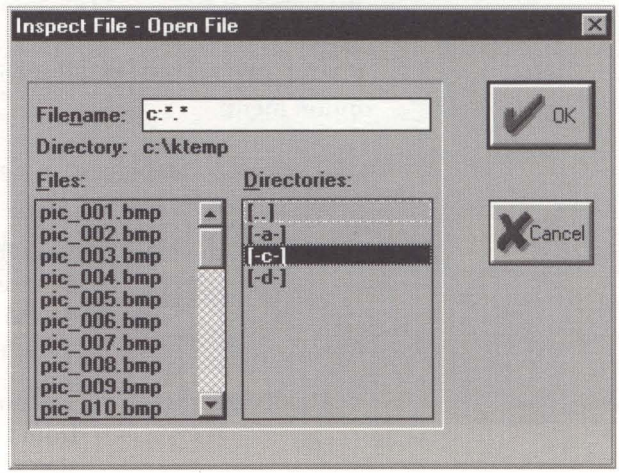
The options available are:

Physical device	Lists the physical devices available. Device 0 is drive A:, device 1 is drive B: and the available hard disks are those numbered 128 and above.
Device geometry	The normal maximum values are read from the BIOS when Inspect Disk is started, but you can override the default settings if necessary.
BIOS default	This sets the cylinder, heads and sectors back to the standard BIOS settings.

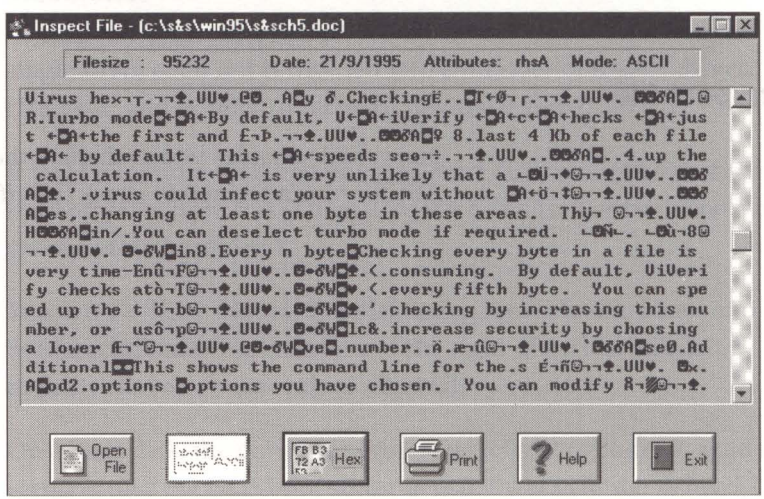
Inspect file

Inspect File enables you to display the contents of a file in either ASCII or hexadecimal to check the effects of a virus.

When you select Inspect file from the Advanced menu, a dialog box similar to the following is displayed:



Select the file you want to examine and click OK. The file contents are displayed in a format similar to the following:



The size of the file, the date it was last changed and its attributes are displayed at the top of the screen.

You can use the scroll bars, the ↓ and ↑ keys, or Pg dn and Pg up keys to scroll through the display if necessary.

You can choose to display the file contents in ASCII or in hexadecimal by selecting the appropriate button. ASCII text is unformatted to allow special characters to be displayed.

You can print the file contents in the currently selected format by selecting Print. You can then choose whether to print the whole file or just the screen display.

If you want to examine another file, select Open File. The file selection box is re-displayed.

5.3 Checking for changes - ViVerify

ViVerify enables you to detect changes in executable files which may be the result of a virus infection. ViVerify works by calculating a unique fingerprint, or checksum, for each file it is protecting. This fingerprint can then be recalculated at any time as a safety check to see if any changes have been made. ViVerify also detects changes in boot and partition sectors.

With this type of tool, you need a balance between speed and security. If the fingerprint calculations are too complex, ViVerify will take a long time to run. On the other hand, if the calculation is too simple, it is possible for a virus to evade detection. This is known as *spoofing*. ViVerify's default settings are a good balance between security and performance. However, you can change the settings if necessary to choose the level of security you want.

ViVerify's default fingerprinting method makes use of a keyword. You have to enter a keyword when the fingerprints are first calculated, and then repeat it every time a check is performed. This increases security by preventing a virus from spoofing the fingerprint.

When to use ViVerify

You can use ViVerify to check executable files regularly.

You can also use ViVerify when cleaning up after a virus infection, as it gives early warning of possible re-infection which can be dealt with before it spreads to other PCs.

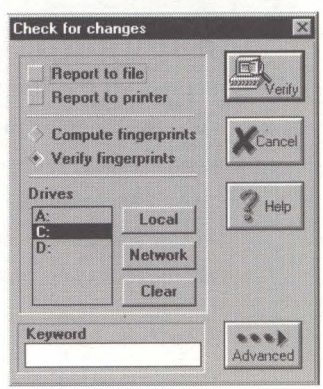
Running ViVerify

You can run ViVerify in two ways:

- From the Toolkit main screen by selecting the Check for Changes box.
- By selecting Check for Changes from the Scan menu.

In both cases the dialog boxes and options are exactly the same.

1. When you select Check for Changes, the following dialog box is displayed:



2. The settings and options are as follows:

Report to — A report of the process always appears on the screen. In addition, you can direct the report to a file, to a printer, or both. If you select Report to file, the report will be saved in a file called VIVERIFY.REP in the default Toolkit folder. (You can change this filename using an

option on the Advanced dialog box.) If you choose Report to printer, the report is sent to your default system printer.

Drives	Select the drives you want to check. Choose Local to scan all the hard drives on your PC. Select Network to check all network drives. Select Clear to clear previous selections.
Keyword	This box only appears when you have selected Compute fingerprints or Verify fingerprints. This is used to encrypt the fingerprints, providing an additional level of protection.

3. These options are suitable for most cases. Additional options can be specified in the Advanced dialog box.

There are two stages in running ViVerify:

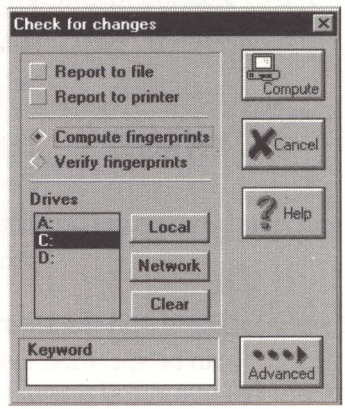
- Firstly, you need to calculate the unique fingerprints for each file, using the Compute fingerprints option.
- Secondly, you can regularly check the set of files for changes, using the Verify fingerprints option.

These two stages are described below.

To compute the fingerprints

To calculate fingerprints for the selected files:

1. Select Compute fingerprints. The dialog box changes slightly:



2. Select the drives to be checked. For example, select Local to make a list for all local hard disk drives.

3. Select the Keyword box. Type in a word of at least eight alphanumeric characters. This keyword is then used as part of the encryption process, which helps prevent a virus from simulating the correct fingerprints.

Note: The keyword is not a password. It is quite safe to write it down and keep it next to the PC - a virus cannot read it!

4. Press the Compute button, or press ↵.

5. When the fingerprints have been calculated, a message is displayed. Press any key (or click the mouse button) to return to the main screen.

Checking the files

Once you have selected the files and computed the fingerprints, you should check them regularly. To check the fingerprints for the selected files:

1. Select Verify fingerprints.
2. Select the drives to be checked. For example, select Local to check the fingerprints for all local hard disk drives.
3. Select the Keyword box. Enter the keyword used previously.
4. Press the Verify button, or press ↵.
5. When the fingerprints have been verified, a message is displayed. Press any key (or click the mouse button) to return to the main screen.

If a file has changed

If ViVerify indicates that a fingerprinted file has been changed, this does not necessarily mean that you have a virus infection. Other possibilities are:

- The changed files could be data files. Data files will always change when they are modified, and occasionally they have names that make them look like executable files.
- Some EXE and COM files are altered by installation routines.
- If ViVerify reports that all programs have been changed, don't panic.

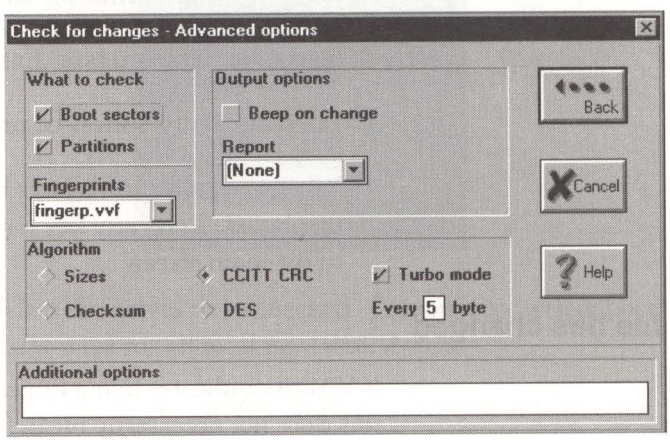
However, if a number of files have changed unexpectedly, it is possible that you have a virus. Make a note of the suspect files, then exit in the normal way from whatever you were doing and save any files you were working on.

Run FindVirus with heuristic checking turned on to check for suspect files. (See "Finding Viruses - FindVirus" on page 39.)

If you have a virus, FindVirus will identify it. Make a note of the details displayed on the report screen. If FindVirus cannot identify a virus in the changed files, it is possible that you have a new virus. See "If you discover a new virus" on page 62.

Advanced menu options

If you select the Advanced box from the Check for Changes screen, a further screen is displayed:



The settings and options are as follows:

Boot sectors — This option is normally selected, and boot sectors are checked on every disk examined. This might cause a problem if, for example, you are checking a network drive which does not have a boot sector. In such a case you can switch this option off.

Partitions — This option is normally selected, and partition sectors are checked on every disk examined. If this causes a problem on a particular disk, you can switch this option off.

Output

If Beep on change is selected, the PC beeps every time ViVerify finds a changed file.

The Report option is only valid if you have opted to send the checking report to a file. If you want to check more than one drive in separate runs, the latest report will overwrite the previous one. Therefore you may want to create a separate report for each drive, for instance C_VER.REP, D_VER.REP, etc. These files are created in the default Toolkit folder unless you specify otherwise.

Algorithm

This box indicates the method used for calculating the fingerprints. The default calculation method is the CCITT Cyclic Redundancy Check, which is suitable for most users.

The Size algorithm calculates fingerprints based on the file size. This is a very fast calculation, but a few viruses do not change the size of files they infect, and therefore can evade it.

The Checksum algorithm calculates the fingerprints as a sum of the bytes checked in the files. The keyword is also incorporated.

The DES option calculates the fingerprints using the standard Data Encryption Standard algorithm, incorporating the keyword. This is very secure but requires lengthy calculations. Only use this option if your company policy requires this level of security.

More details on encryption methods are given in Chapter 10, "Advanced Virus Checking".

Turbo mode	By default, ViVerify checks just the first and last 4 Kb of each file by default. This speeds up the calculation. It is very unlikely that a virus could infect your system without changing at least one byte in these areas. You can deselect turbo mode if required.
Every n byte	Checking every byte in a file is very time-consuming. By default, ViVerify checks every fifth byte. You can speed up the checking by increasing this number, or increase security by choosing a lower number.
Additional options	This shows the command line for the options you have chosen. You can modify this directly if you wish. Full details of the various parameters and switches are given in Chapter 10 "Advanced Virus Checking".

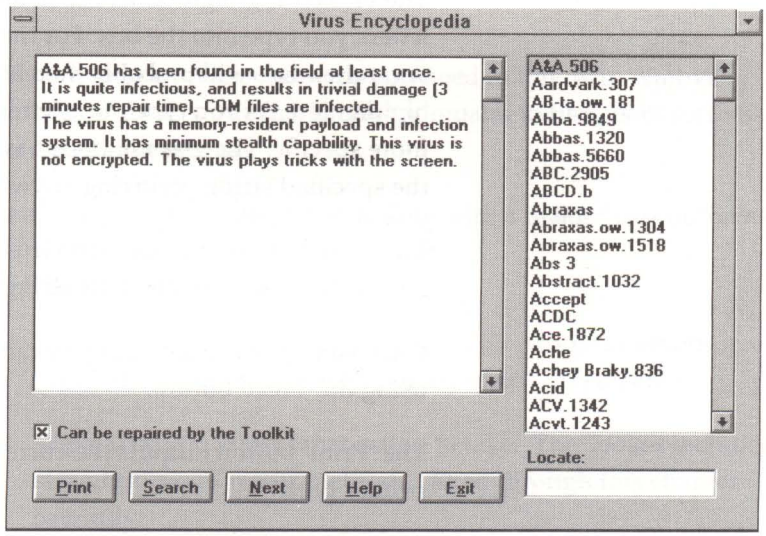
You can save the changed ViVerify settings for future use. Select Save Configuration from the File menu. For more information, see Chapter 11, "Toolkit Configuration".

5.4 The Virus Encyclopedia

The on-line Virus Encyclopedia contains details of all the viruses recognized by the Toolkit. You can view the Encyclopedia in two ways:

- From the Toolkit main screen by selecting the Virus Information button.
- By selecting Virus Encyclopedia from the Advanced drop-down menu.

The following screen is displayed:



For the virus highlighted in the 'Viruses' list on the right hand side of the dialog, the 'Description' provides the following information:

- How common it is.
- How infectious it is.
- How much damage it does.
- What is infected: files, boot sectors or partition sectors.
- Whether or not it has memory-resident capabilities.
- If it uses stealth.
- If it is polymorphic.
- Any aliases it is known by, and whether there are any variants.

A virus can be highlighted in the 'Viruses' list by clicking on it with the mouse. Keyboard users can move the selection bar using the cursor keys.

Use the 'Locate' box to jump to a specific part of the 'Viruses' list. The virus is highlighted whose name starts with the string of letters you type into the box. For the first few letters you type several viruses will probably match; the first one in the list will be highlighted. As you type more letters the identification will get more specific. The 'Search' option is more powerful as it can find the specified string occurring anywhere in the virus name.

The 'Search' button finds each virus whose name, or the name of any of its aliases, contains the string of letters you enter.

Once you have run a search you can step to the next found match using the 'Next' button.

The 'Print' button outputs the current description to the default printer port.

6. Virus Repair and Removal

This chapter explains the steps you need to follow to remove viruses and carry out any necessary repairs to files, boot sectors and partition sectors.

It also suggests a strategy for dealing with a major virus outbreak.

If you have discovered a virus:

- Don't panic. More damage is caused by people attempting to repair the problem wrongly than by viruses themselves.
- Make sure you know what action to take. The Toolkit includes straightforward repair methods. Read through this chapter carefully.
- If you are in any doubt, leave the computer turned off.
- If your company has procedures for dealing with viruses, you should follow them.

6.1 If you find a Virus

Are you sure you have a virus?

- If ViVerify has reported suspect files, this does not necessarily mean you have a virus. Run FindVirus with heuristic checking on to check suspect files. If you have a virus, FindVirus will identify it. See "Finding Viruses - FindVirus" on page 39.
- If FindVirus reports a named file virus or a diskette boot sector virus, you can repair it easily with the Windows 95 Toolkit. See "Single button repair" on page 61.
- If FindVirus reports suspect files, but does not name a virus, you may have discovered a new virus. See "If you discover a new virus" on page 62.

- If FindVirus finds a virus in the boot or partition sector of a hard disk, you cannot repair it using the Windows 95 Toolkit. Proceed as follows:

  - Boot from a clean, write-protected, DOS system diskette.

  - At the system prompt, insert the diskette containing FINDVIRU.EXE from the DOS Toolkit into the appropriate drive (the DOS Toolkit is supplied with the Windows 95 Toolkit

  - Change to that drive by typing `A:` or `B:` and pressing ↵.

  - Type `FINDVIRU /REPAIR /LOCAL` and press ↵.

  - The screen displays a list of the files infected. Where possible, files are repaired, otherwise they are renamed.

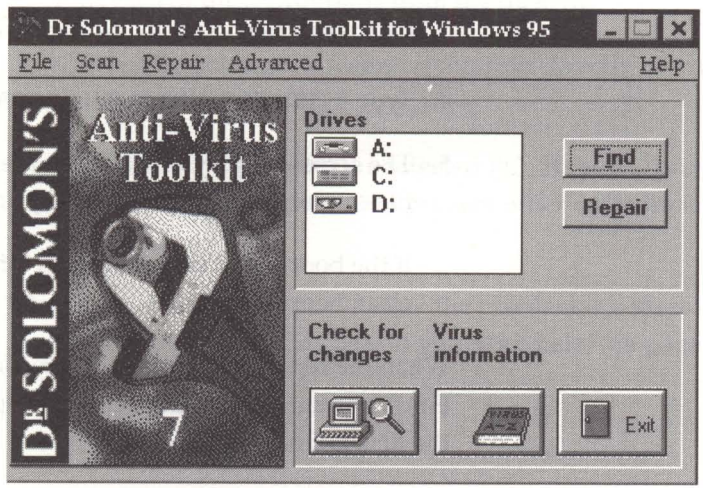
  - If the boot sector of a diskette is infected, it is replaced with a clean boot sector.

  - Documentation supplied with the DOS Toolkit contains full details. If you are in any doubt, contact Dr Solomon's Support staff. See "If you need help" on page xiv.

6.2 Single button repair

The Toolkit includes a straightforward facility for repairing infected files and diskette boot sectors.

The single-button repair can be run from the main screen:



In the Drives box, select the drive on which you have found a virus, then select Repair.

The repair program operates as follows:

1. Any infected files are repaired, if possible. If a file cannot be repaired, it is renamed. The first character of each file extension is changed to a V. For example COM is changed to VOM and EXE to VXE.

2. If the boot sector of a diskette is infected, it is replaced with a clean boot sector.

The Repair program cannot repair infected boot sectors or partition sectors on hard disks. You need to reboot your system under DOS and use the DOS version of the Toolkit.

To repair an infected hard disk boot sector or partition sector:

1. Boot from a clean, write-protected, DOS system diskette.
2. At the system prompt, insert the diskette containing FINDVIRU.EXE from the DOS Toolkit into the appropriate drive.
3. Change to that drive by typing `A:` or `B:` and pressing ↵ .
4. Type `FINDVIRU /REPAIR /LOCAL` and press ↵ .
5. The screen displays a list of the files infected. Where possible, files are repaired, otherwise they are renamed.

   If the boot sector of a diskette is infected, it is replaced with a clean boot sector.

When the repair is complete, it is recommended that you run FindVirus again, with the heuristics option selected, to check that the disk is free from viruses.

6.3 If you discover a new virus

You may have discovered a new virus in the following situations:

- If you have run FindVirus with heuristic scanning switched on and suspect files have been found.
- If ViVerify notifies you of a changed file, but FindVirus does not find a recognized virus.

If you suspect a new virus:

1. Boot normally and format a diskette in the infected computer.
2. Copy any files that you suspect are infected to the diskette.

3. Copy the following additional files to the diskette:

   MEM.EXE
   CHKDSK.COM
   DISKCOPY.COM
   MODE.COM

   Run each of these programs from the diskette.

4. Contact Dr Solomon's Technical Support directly, or your authorized distributor.

5. Do not run anything on the infected PC. If the PC is attached to a network, disconnect it to prevent other users from accessing any files.

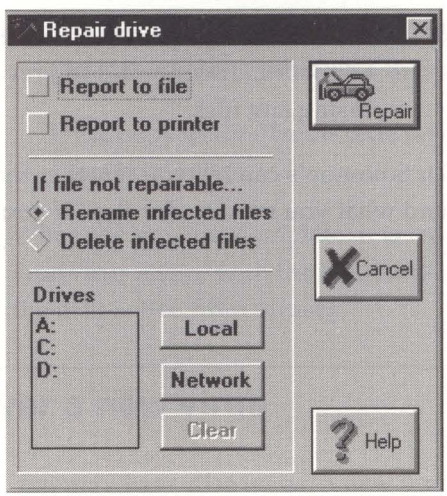
Dr Solomon's can tell you whether the problem is a virus or not, and what you need to do. See "If you need help" on page xiv.

6.4 Repair menu options

As an alternative to the Repair button, you can repair files and diskettes from the Repair menu.

Repairing drive

You can repair infected files using the Repair drive option on the Repair menu. This runs FindVirus to find and repair viruses. The following screen is displayed:



The settings and options are as follows:

Report to	A report of the repair process is displayed on the screen. In addition, you can direct the report to a file, to a printer, or both.
Drives	Select the drives you want to scan. Choose Local to scan all the hard drives on your PC. Select Network to scan all network drives. Select Clear to clear any selections you have made.

If file is not repairable

By default, if a file cannot be repaired, FindVirus renames it to prevent someone from running it accidentally. The first letter of the file extension is changed to a V. For example, FORMAT.COM is changed to FORMAT.VOM.

If you set the Delete infected files option, FindVirus will delete any files that cannot be repaired.

Files are overwritten before deletion to ensure that they cannot be recovered by an Undelete program.

When all the settings are correct, select Repair. FindVirus scans the specified drives and attempts to repair any infected files.

Note that when FindVirus is run with the Repair option it scans all files, including data files and macro files. This is in case an executable file has been renamed with a different file extension, and because macro viruses exist. It also scans files that have been compressed using PKLite, PKARC, PKZIP, ICE, LZExe, DIET, LHA, CRYPTCOM or ARJ.

FindVirus produces a report detailing the action taken. If any files cannot be repaired, you must restore the original clean copies from backups.

Replacing diskette boot sectors

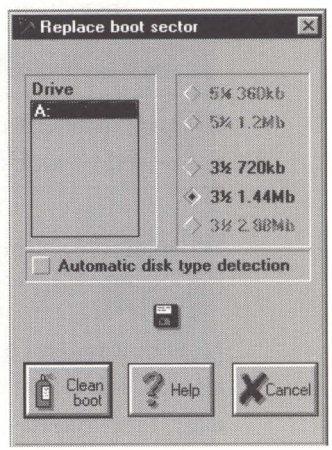
You can replace an infected boot sector on a diskette with a valid, non-infected boot sector using the Replace boot sector option on the Repair menu.

The single-button repair facility will also replace diskette boot sectors. See "Single button repair" on page 61.

This tool does not delete the boot sector virus, but overwrites the entire boot sector so that the diskette is no longer infected.

Replace boot sector works on 5¼" diskettes of 360 Kb and 1.2Mb capacity, and on 3½" diskettes of 720 Kb, 1.44 Mb and 2.88 Mb capacity.

Place the diskette you want to repair in the drive and select Replace boot sector from the Repair drop-down menu. The following screen is displayed:



The system automatically detects the number and type of diskette drives on the PC. Select the appropriate drive in the Drive box.

Select the size and capacity of the diskette to be repaired. If you are not sure of the diskette capacity, select Automatic disk type detection. The system then checks the diskette type itself.

Select OK to replace the boot sector.

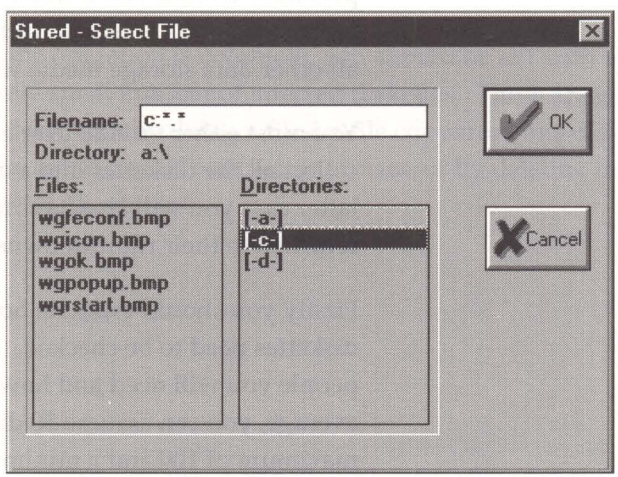
If the virus has made other changes to the diskette, apart from overwriting the boot sector, these will not be undone by running Replace boot sector. For example, if the virus has created fake bad sectors to store part of itself, those bad sectors will still be there. However, the diskette is safe to use, as code in those sectors can no longer be executed.

6.5 Shredding files

If FindVirus has been unable to repair an infected file, and has changed the first letter of the file extension, you should restore a clean copy from backup and delete the renamed file. To ensure security, it is safer to use the Shred program to delete those infected files.

Shred overwrites a file with a series of characters, and then deletes it. In this way the file cannot be recovered using an Undelete program.

Select Shred from the File menu. The following file selection box is displayed:



Select the file to be shredded, and select OK. You are asked to confirm the action, since you are not able to restore the file. The file is overwritten and then deleted.

6.6 Eradicating a virus

If you have a major virus outbreak in your organization, it is essential that you find and clean up all the infected systems and media. If you leave out just one diskette or workstation, you will soon be back to where you started.

This is not a trivial problem when many PCs are involved.

This section gives details of a suggested strategy for cleaning up after a virus outbreak in an organization.

Planning the clean-up

Before starting the clean-up you must estimate the size of the problem. Even if you think that only a small percentage of PCs are infected, it is essential to check every PC, every diskette, and all other data storage media within the company.

You must either visit all user areas and check the media in situ, or collect all the diskettes into a central checking location. In the latter case you will also have to ensure that all diskettes are returned to their rightful owners.

Firstly you should estimate how many PCs and how many diskettes need to be checked. You can then work out how many people you will need and how long the operation will take. On average, you can assume 50 diskettes per computer, with a maximum of 100 and a minimum of 25.

You will need several PCs to scan the diskettes. Make sure you have 3½" and 5¼" drives if you use both types of diskette. Obviously, you need to make sure the PCs used for checking are clean first!

If there are several thousand diskettes to be checked, it may be worthwhile hiring or buying a diskette autoloader. A special version of the Toolkit is available which will run on a PC connected to an autoloader. For more information, call Dr Solomon's Software or your authorized distributor.

Once you know the size of the task, you can organize the staff you need.

Checking diskettes

If the diskettes are readable, run FindVirus to scan for viruses and then run the Repair options to repair infected files and sectors. If there is any uncertainty, the diskette should be put aside for a final check.

Diskettes which pass the final check should be returned to the diskette controller for return to the user. All checked diskettes should be write-protected, and marked to show that they are clean. This is mainly to give users confidence that their diskettes have been checked.

Checking PCs

When the operation is complete, you should be left with a relatively small number of infected diskettes. These are generally easily dealt with by doing a file-by-file copy from one diskette to another, in the case of boot sector viruses, or by deleting the file in the case of file viruses.

This page has been left blank.

7. Using the Scheduler

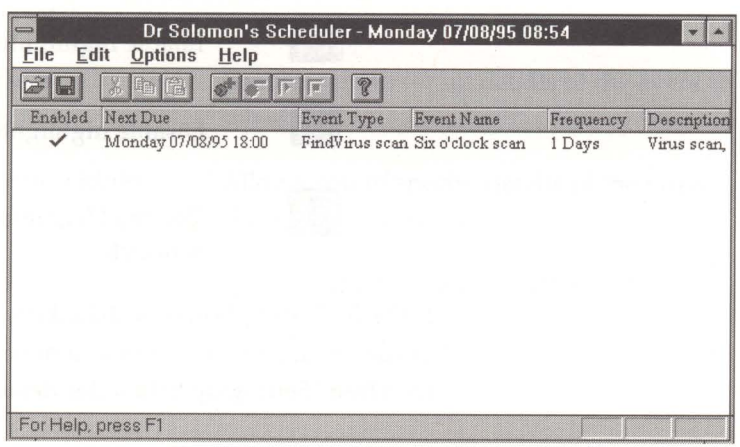
This chapter explains how to use the Scheduler which is provided in the Anti-Virus Toolkit for Windows 95. This facility allows you to scan your hard disks for viruses, using FindVirus, at any time, even while your PC is unattended. You can also use the Scheduler to run any application on a regular basis, and to send messages to any other users on your network.

To use the Scheduler, you need to use the Schedule Editor to create an event detailing the program to be run and the time details. Then launch the memory-resident Scheduler which will start up your events at the pre-set times.

You can perform an event once, at a pre-determined time, or you can run it at regular intervals. For example, you can run FindVirus every week to search your hard disks. Details of events performed can be written to a log file, so you can check the results.

7.1 The Schedule Editor

To check the current schedule, select Schedule Editor directly from the Anti-Virus Toolkit program group. A screen of the following format is displayed:



This screen summarizes any events you have already set up. The Enabled column indicates whether or not this event is scheduled to run.

To create new events or make amendments, you can either choose options from the drop-down menus or click on items on the toolbar running along the top of the screen. The toolbar icons are as follows:

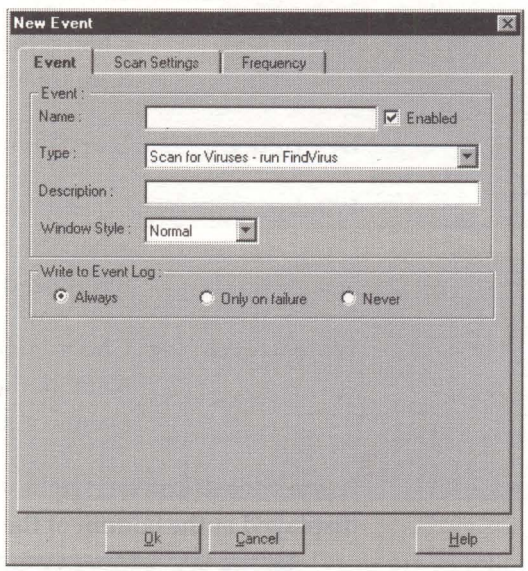
Toolbar icon	Purpose
	Open previously saved event file.
	Save current event file.
	Cut selected text and place on clipboard.
	Copy selected text to the clipboard.
	Paste text from the clipboard.
	Add new scheduled event.
	Delete highlighted event.
	Enable highlighted event.
	Disable highlighted event.
	Display Help information about the Scheduler.

If the Tooltips option is switched on, a box explaining the purpose of each icon appears when you move the cursor to a particular icon (see "Setting up Scheduler defaults and options" on Page 79).

7.2 To set up a new event

Once you have set up a new event as described below, you must make sure that the Scheduler is running before the event can take place; see "Running the Scheduler" on Page 78.

Select Add New Event from the Edit menu, or select the Add Event icon. The following screen appears:



The three tabs at the top of the screen allow you to set up the event.

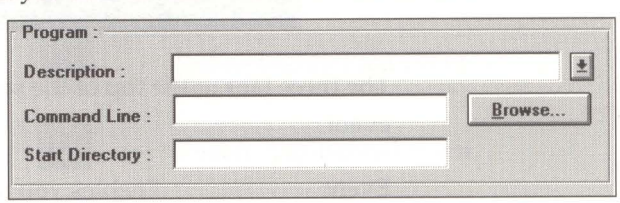
Event	Enables you to set up details of the event to be scheduled.
Scan settings	Allows you to specify details of the virus checks to be carried out.
Frequency	Specifies the frequency of the event.

Setting the event details

On the Event screen, the settings and options are as follows:

Name	Identify the new event. The Name appears on the schedule and the event log, so make sure it identifies the event and is unique.
Enabled	Select Enabled to ensure the event is run. Clear Enabled to prevent the event from running
Type	Choose the type of event to be performed - Scan for Viruses or Run an Application.
Description	Enter some explanatory text, if you wish.
Window style	Choose how the relevant window is to appear when the event runs - normal, maximized, minimized or hidden.
Write to event log	Choose whether or not to record details of the event in the Toolkit log file. You can record all events or just those that fail.

If you choose Run an Application some additional information is displayed at the bottom of the Events screen:

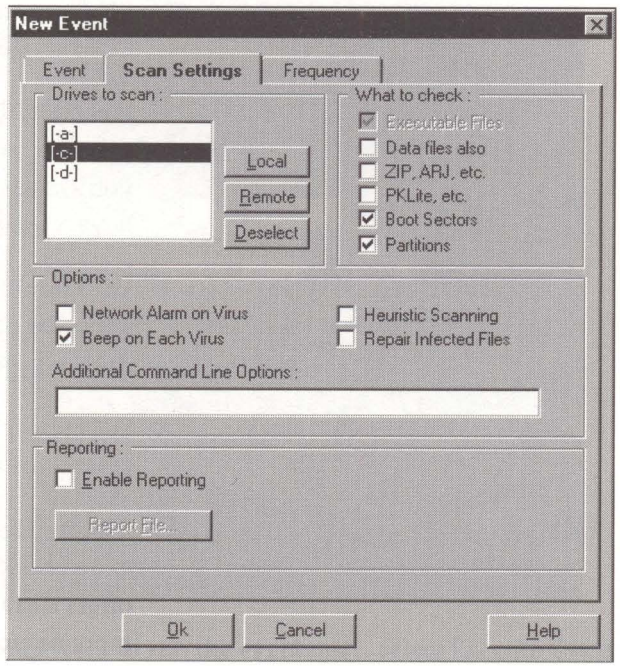


Description	Select the program to be run from the drop-down list, if you have already set it up as a default. See "Setting up Scheduler defaults and options" on Page 79. Alternatively, you can enter a Description directly.

The Command Line and Start folder appears automatically if you have chosen a default. Otherwise, press Browse to find and select the program.

Scan settings

If you are scheduling FindVirus, you need to choose the Scan Settings tab. (This tab is not available when scheduling other events.)



The settings and options for FindVirus are as follows:

Drives to scan — Choose Local to scan all the drives on your PC. Choose Remote to scan all the remote drives. Press Deselect to remove a selection.

What to check — By default, FindVirus scans files most susceptible to virus infection, boot sectors and partition sectors. You can change these settings if you wish.

Select Data files also to scan all non-executable files.

Select ZIP, ARJ to scan files which have been archived using utilities PKZIP, PKARC, LHA or ARJ.

Select PKLite if you want FindVirus to scan files compressed by utilities PKLite, ICE, LZExe, DIET or CRYPTCOM.

You should only deselect Boot sectors if this causes a particular problem; for example, if you are scanning a network drive that doesn't have a boot sector.

You should only deselect Partitions to suppress partition sector scanning when this causes a problem.

Options

Select Beep on Each Virus if you need this extra warning when a virus is found.

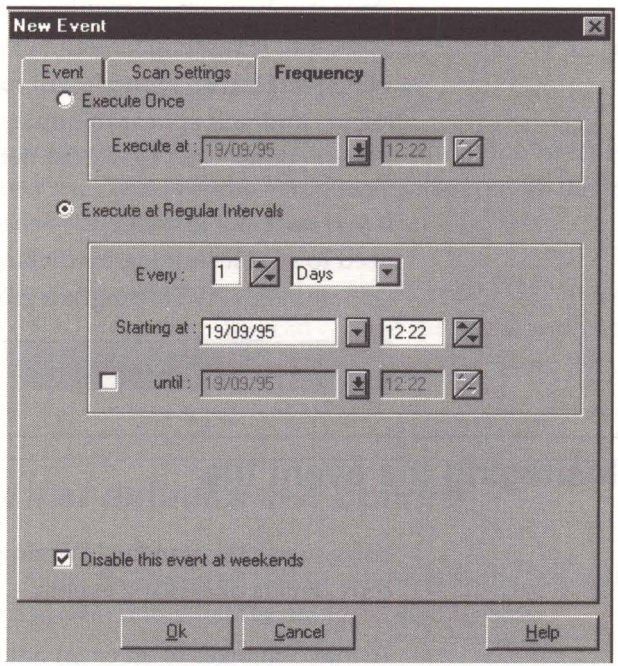
Choose Heuristic Scanning if you want to run extra checks for potential new viruses. This offers extra protection for users who need more security, but can increase scanning times by approximately 50%.

Choose Repair Infected Files if you would like any infected files to be repaired automatically.

Although FindVirus can detect hard disk boot sector and partition sector viruses, it cannot repair them automatically. You need to reboot your PC under DOS and run the DOS Anti-Virus Toolkit. For more information, see Chapter 6, "Virus Repair and Removal".

Frequency settings

For all types of events, you need to set the Frequency options.



If you only want to run the event once, select Execute Once. Then enter the date and time that the event is to be run.

If you want to run the event on a regular basis, select Execute at Regular Intervals. Enter the frequency, for example, Every 2 Days or Every 4 Weeks. Enter the date and time that you want the event to start. If you wish, you can also enter an end date and time.

If the event is only to run on weekdays, select Disable this event at weekends.

You can type dates and times directly, or you can use the Windows buttons to change the default entries.

7.3 Running the Scheduler

Once you have set up regular events, you need to make sure the Scheduler is running. If you have installed the Scheduler in the Windows Startup group it will run automatically whenever you log on, and will appear minimized in the tool bar. See "Installing the Scheduler" on Page 21 for details.

If you have not installed the Scheduler in the Startup group, you need to start it running by clicking on the following option in the Dr Solomon's AVTK program group:.

7.4 Managing the event file

You can use the standard Windows cut and paste functions to copy details of existing events.

To make changes to an event after you have set it up, either highlight it in the event list and select Edit Event from the Edit menu or simply double-click on the event.

If you want to temporarily prevent an event from running, select the Disable icon (or clear the Enable check box on the Event screen). To resume it, click the Enable button.

The event file is stored as TK_SCHED.SDF. If you edit this file with a text editor, you can run Validate from the File menu to check the syntax and delete any invalid entries directly.

The options for saving the event file depend on the defaults set up. See "General defaults" on Page 80 for details. To save the existing event file immediately, select Save from the File menu. To discard changes you have made and reload the previously saved event file, select Reload from the File menu.

7.5 The Toolkit Event Log

Depending on the settings you have included on the event screen, information may be written to the log file whenever an event is performed, or when an event fails to run.

To check the log file, select Event Log file from the File menu, then choose View. This will run Windows Notepad with the log file loaded so you can check the event.

By default, the log file is saved as TK_SCHED.LOG in the C:\WINDOWS folder. You can change the name and path if you wish, by selecting Event Log file from the File menu, then Change Name.

7.6 Setting up Scheduler defaults and options

The Options menu allows you to choose how the Scheduler screens appear and what the standard settings are.

The Font option allows you to change the typeface and size used when the event file is displayed.

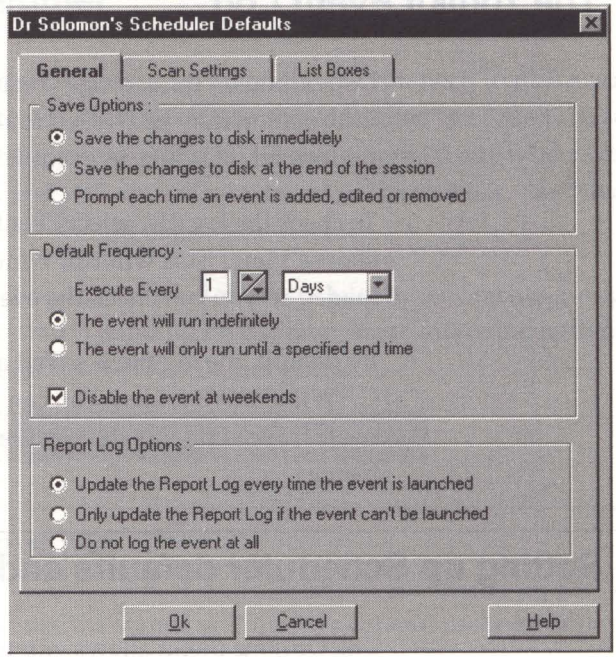
If you select Show Toolbar, the toolbar appears at the top of the screen. This offers an alternative way of choosing the options.

If you select Show Status Bar, the status bar at the bottom of the screen appears.

If you select Show Tooltips, a box explaining the purpose of each icon appears when you move the cursor to a particular icon.

The Defaults option on the Options menu allows you to set the default values for the various Scheduler screens.

If you choose this option, the following screen appears:


Dr Solomon's Scheduler Defaults
General
Scan Settings
List Boxes
Save Options :
Save the changes to disk immediately
Save the changes to disk at the end of the session
Prompt each time an event is added, edited or removed
Default Frequency :
Execute Every
1
Days
The event will run indefinitely
The event will only run until a specified end time
Disable the event at weekends
Report Log Options :
Update the Report Log every time the event is launched
Only update the Report Log if the event can't be launched
Do not log the event at all
Ok
Cancel
Help

The three tabs at the top of the screen allow you to select the various categories of defaults. Select OK when you have finished.

General defaults

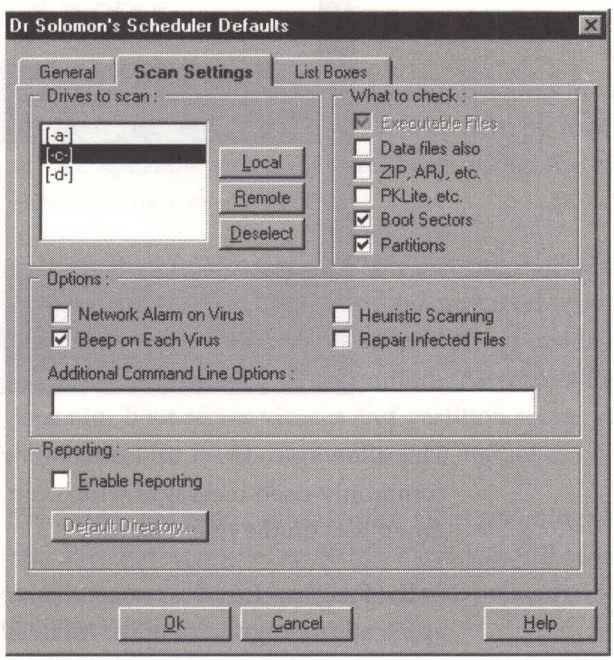
On the General defaults screen the settings are as follows:

Save Options	Choose whether changes to the event file should be saved straight away, when you have finished using the Schedule Editor, or whether a prompt should be issued whenever a change is made.
Default Frequency	Set up the default values that will appear on the Frequency screen.
Report Log Options	Set up the default for writing events to the event log.

Remember these are the default values that appear on the screen when you set up new events. You can always change them to suit your specific requirements.

Scan Settings

If you choose the Scan Settings tab, the following screen appears:

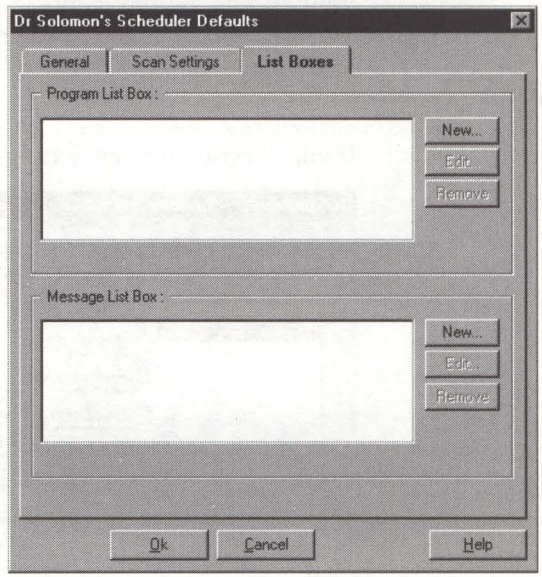


Set up the FindVirus settings that you are most likely to use. The settings are described in "Scan settings" on Page 75.

Remember these are the default values that appear on the screen when you set up new events. You can always change them to suit your specific requirements.

List Boxes

If you choose the List Boxes tab the following screen appears:



This allows you to set up frequently-run programs and commonly-used messages which can then be selected from drop-down lists on the Event screen.

In the Program List Box, select the New button to choose a new application program to add. All available programs are listed, and you can browse through and pick the one that you want.

In the Message List box, select New to enter a new message.

In both boxes you can edit or delete existing entries by highlighting the entry and choosing the appropriate button.

8. Advanced Virus Detection

This chapter includes technical information on using FindVirus, including details of all the options and tips on running the program from within batch files.

8.1 How FindVirus works

FindVirus scans your hard disks and diskettes for all the viruses listed in a virus driver file. It detects them by scanning the files for recognizable strings of bytes from within the virus code, and other sophisticated methods.

By default, FindVirus scans files most susceptible to virus infection, including system, hidden and read-only files, but it can also be configured to scan all data files and inside compressed files. Long filenames are supported. As well as file viruses, it looks for boot sector viruses and partition sector viruses. FindVirus also finds common trojans and jokes.

FindVirus has been optimised for virus scanning, so it works very quickly. For example, an 80 Mb hard disk full of executable files can be scanned in about 20 seconds. Obviously, the faster the PC, the faster FindVirus works.

FindVirus can be run from the Scan drop-down menu, or directly from the main screen by selecting Find. Details of using it in this way are given in Chapter 5, "Checking for Viruses".

Because it scans for the specific viruses within the virus driver file, it is vital that this file is kept up-to-date. If your version is out-of-date, a message is displayed to that effect when you run FindVirus. See "Registration and upgrades" on page xiii.

Executable files

File viruses only infect executable files and data files containing macro code. By default, FindVirus scans for files with the following extensions:

APP	DOT
BAT	EXE
BIN	OV?
CMD	QLB
COM	SYS
DEV	XTP
DLL	001
DOC	002

If you have vulnerable files with other extensions, you should set FindVirus up to scan for all files. In its default mode, FindVirus scans files with the above extensions in every folder on a disk.

Compressed and archived files

FindVirus can scan for viruses in files that have been compressed using many common archiving programs. It achieves this by decompressing as much of the files to memory as necessary and then scanning them for viruses. Because the PC's available memory is used to decompress files, it does not need any hard disk space or access to diskettes. FindVirus can scan files compressed using the following tools:

ARJ	LZExe
CRYPTCOM	PZARC
DIET	PKLite
ICE	PKZIP
LHA	Microsoft Expand

Others will be added in future releases.

By default, scanning of compressed files is turned off.

FindVirus can also scan inside "unextractable" PKLited files.

Self-extracting archived files, such as those created with the PKWare utility ZIP2EXE, can also be scanned. FindVirus does not support multi-disk archives.

If you have multiple-level archived files, such as ARJ files within ZIP files, FindVirus recursively decompresses all levels and scans them completely for viruses if enough memory is available.

When scanning compressed executable files, FindVirus reports that it has scanned the self-extractor code and then that it has scanned the contents of the compressed file. This does not mean that the same file is scanned twice.

If you have compressed files which have been encrypted with passwords, FindVirus is unable to scan them for viruses. In these instances it displays a message at the end of the scan warning that password-encrypted files were found and have not been scanned. For complete security you should unpack these files manually and decrypt them before scanning them.

Scanning compressed and archived files slows down FindVirus and is really only necessary for sheep-dip PCs.

Repairing files

FindVirus can also be run with the Repair option, to remove viruses and repair executable files. It attempts to remove any viruses and restore the files.

For more information, see Chapter 6, "Virus Repair and Removal".

8.2 Running FindVirus from the user interface

You can run FindVirus from the user interface in the following ways:

- From the main screen, by choosing the drives to be scanned and selecting Find.
- By selecting Find Viruses from the Scan menu.

These options are explained in detail in Chapter 5, "Checking for Viruses".

8.3 Running FindVirus from the command line

You can run FindVirus from a command line by clicking Start, selecting the Run option and entering the command in the Open: box. You can also include the appropriate commands within a batch file.

Syntax

The command syntax is:

```
WFINDV32 [switches]
```

The switches are as follows:

Switch	Meaning
`/ALLDRIVES`	Scan all fixed disk drives, including network drives.
`/ANALYSE`	Run heuristic analyser, to look for possible new viruses.
`/BADLIST=`*`file`*	Write suspect filenames to the specified file.
`/BEEP`	Beep when a virus is found.
`/CHECKLIST=`*`file`*	Scan files listed in specified file.

Switch	Meaning
`/D=drives`	Scan specified drives.
`/DOALLFILES`	Scan all files, not just executables.
`/DRIVER=`*`file`*	Use named virus driver file.
`/EXTERROR`	Provide extended error levels.
`/EXTRA=`*`file`*	Use named additional virus driver.
`/FORCEFLOPPY`	Force reading of diskette boot sector when diskette is changed.
`/HELP` `/?`	Display the most common FindVirus switches.
`/INI`	Read parameters from INI file
`/LOCAL`	Check local hard disk drives.
`/LOUD`	Display status of each file scanned.
`/NOBOOT`	Do not scan boot or partition sector.
`/NOFILES`	Disable file scanning.
`/NOPACK`	Do not scan files compressed with PKLite, LZExe, ICE, DIET or CRYPTCOM.
`/NOPART`	Do not check partition sectors.
`/ONEONLY`	Check one diskette only.
`/ONVIRUS="`*`msg`*`"`	Display the specified message if a virus is found.
`/PACK`	Scan files compressed with PKLite, LZExe, ICE, DIET or CRYPTCOM.
`/PAUSE`	Pause for keystroke before scanning.
`/PRINTOUT`	Output report to the printer as well as to the screen.
`/REPAIR[/DELETE]`	Repair infected files. The optional `/DELETE` switch deletes files that cannot be repaired.

Switch	Meaning
/REPORT=*file*	Output report to specified file.
/SUMMARY	Produce a summary report.
/UNPACK	Scan compressed files. (Superseded by /UNZIP and /PACK.)
/UNZIP	Scan files compressed with PKARC, PKZIP, ARJ, PKLite, LZExe, ICE, DIET, LHA or CRYPTCOM.

The action of the switches is discussed in the following sections. You cannot use any switch more than once on the command line. For example, only the first /LOCAL has any effect. The switches must be separated by spaces and can be in upper or lower case. You can display the most common switches by running WFINDV32 with the /? or /HELP switches.

Scanning specific drives

The most common way of defining the drive to be scanned is to specify the drive on the command line. For example, to scan the C: drive, use:

```
WFINDV32 C:
```

Alternatively, you can use one of the following switches:

```
/D=
/ALLDRIVES
/LOCAL
```

If you do not specify a drive, FindVirus prompts for the drive to be scanned.

The /D= switch allows you to specify one or more specific drives.

/D=*drive* Scans the specified drive(s).

For each drive you want to scan, enter the identifying letters, with colons and separated by semicolons. For example:

```
WFINDV32 /D=C:;D:
```

scans the C: and D: drives.

`/ALLDRIVES`	Scans all fixed disk drives, including network drives.
`/LOCAL`	Scans the current local hard disk drives.

If you specify a diskette drive, FindVirus will automatically scan a number of diskettes in the same drive. For example:

```
WFINDV32 /D=A:
```

Once each diskette has been scanned, you will be prompted to remove it and insert the next. You can change this default with the following switches:

`/ONEONLY`	Scans one diskette only, and does not prompt for further diskettes.
`/PAUSE`	Pauses after loading a diskette.

For example:

```
WFINDV32 /D=A: /ONEONLY
```

scans just one diskette in drive A:, and does not prompt for further diskettes.

Scanning files and folders

By default, FindVirus scans all executable files on the specified drive. You can specify particular files to be scanned with a number of switches.

To scan data files as well as executables, use the `/DOALLFILES` switch. For example:

```
WFINDV32 /LOCAL /DOALLFILES
```

scans all files (executable and data) on the local hard drive.

By default, FindVirus scans the files normally attacked by viruses. These are executable files and data files that use complex macro languages. Use `/DOALLFILES` when cleaning up after a virus infection or on a 'sheep-dip' machine.

If you want to scan a particular set of files, you can use the `/CHECKLIST` option:

`/CHECKLIST=`*`file`* Scans only the files listed in the specified file.

You can create a file containing the names of the files you want FindVirus to scan using a text editor or word processor. This must be an ASCII file containing only the filenames, including extensions, one filename on each line. Do not include drive or path specifiers.

You can also use this option to scan suspect files included in a list produced by ViVerify with the `/BADLIST` option.

For example:

```
WFINDV32 /CHECKLIST=SUSPECT.LST
```

scans just those files listed in SUSPECT.LST. If a pathname is not given, the file is assumed to be in the default Toolkit folder.

By default, FindVirus does not scan any compressed and archived files. If you want to scan these files, use the `/UNZIP` and `/PACK` options.

`/PACK` Scans files which have been compressed using the PKLite, LZExe, ICE, DIET or CRYPTCOM utilities.

`/UNZIP` Scans files which have been archived or compressed with PKARC, PKZIP, PKLite, LZExe, ARJ, ICE, LHA, DIET, Microsoft Expand or CRYPTCOM utilities.

`/NOPACK` Turns off scanning files compressed with PKLite, LZExe, ICE, DIET or CRYPTCOM. This is the default setting.

For example:

```
WFINDV32 C: /NOPACK /UNZIP
```

enables the scanning of archived files (such as PKZIP and ARJ) but not compressed files (such as PKLite and LZExe).

Scanning compressed and archived files may increase scanning time as files have to be decompressed first.

Scanning boot and partition sectors

By default, FindVirus scans boot and partition sectors on every disk. You can turn these checks off, but this is recommended only if an option is causing a problem; for example, if you are scanning a network drive which does not have a boot sector.

`/NOBOOT` Stops FindVirus scanning the boot and partition sectors of the disk(s) specified.

`/NOPART` Stops FindVirus scanning the partition sector of the disk(s) specified.

Producing reports

By default, FindVirus displays a report on the screen when it has finished its scan. A number of additional reporting options are available.

`/PRINTOUT` Directs the report to the default system printer as well as to the screen.

`/REPORT=`*`file`* Directs the report to the specified file as well as to the screen. The `/APPEND` switch appends the report to an existing file. If you only give a filename, the file is created in the default Toolkit folder.

`/LOUD`	Provides a more detailed report. As each file is scanned, the result is displayed on the screen.
`/BADLIST=`*`file`*	Writes the names of suspect files, together with viruses, to the specified file. If you only give a filename, the file is created in the default Toolkit folder. To save it elsewhere, give a full pathname.

For example:

```
WFINDV32 C: /REPORT=VIRUS.REP /LOUD
```

scans the C: drive for viruses. As each file is scanned, its name is displayed on the screen. This detailed information is also written to a file called VIRUS.REP in the Toolkit folder.

Identifying viruses

`/ANALYSE`	Runs a heuristic scanner, looking for suspicious code that may be a warning of a new virus.

Use this option if you need extra security, for example if you use a large number of diskettes. It will increase scanning time.

Specifying actions

Switches can be set to request particular actions during or after a scan.

`/BEEP` Sounds a beep whenever a virus is encountered. By default, one beep is sounded at the end of the scan if any viruses have been detected.

`/ONVIRUS="`*`message`*`"` If this switch is set, FindVirus displays a message. The message must be in quotation marks and can contain any character except double quotation marks (") and forward slash (/), to a maximum of 40 characters.

For example:

```
WFINDV32 /LOCAL /ONVIRUS="Virus found.  Call PC
Support on 1234"
```

scans all local drives for viruses. If a virus is found, the warning message is output to the screen.

Defining drivers

When scanning, FindVirus uses a virus driver file called FINDVIRU.DRV which contains details of all current viruses. It also checks for an additional driver file called EXTRA.DRV which may contain details of more viruses. If additional drivers are provided by Dr Solomon's, for example as an upgrade, you may need to use one of the following switches.

`/DRIVER=`*`file`* Instructs FindVirus to use the named virus driver file instead of FINDVIRU.DRV.

`/EXTRA=`*`file`* Instructs FindVirus to use the named additional driver file as well as FINDVIRU.DRV.

Extra driver files are available from Dr Solomon's Bulletin Board. See "If you need help" on page xiv for contact details.

Repairing files

To repair infected files, you can run FindVirus with the `/REPAIR` option.

Note: The Repair button on the user interface provides a straightforward way of repairing files, boot sectors and partition sectors. See Chapter 6, "Virus Repair and Removal".

`/REPAIR` Runs the repair options. If a virus is found, FindVirus attempts to repair the file. If the virus cannot be removed, the infected file will be renamed to prevent accidental use. For example, EXE files will be renamed with VXE extensions. Infected boot and partition sectors are also repaired.

`/DELETE` The `/DELETE` switch causes FindVirus to delete any files that cannot be repaired, rather than renaming them. Before deleting the files, FindVirus overwrites them with zeroes to prevent anyone recovering them with an UNDELETE tool. You can only use the `/DELETE` switch in conjunction with the `/REPAIR` option.

For example:

```
WFINDV32 /LOCAL /REPAIR /DELETE
```

scans all local hard disks for viruses, and attempts to repair any infected files found. If any infected files cannot be recovered, they will be deleted. FindVirus will prompt for confirmation before deleting each file.

Scanning backup files

If you use FastBack or PCTools to make backups, FindVirus might report that the backup diskettes cannot be read. Because of the formatting, DOS cannot read the boot sector or any of the files on these diskettes.

If you have had a virus outbreak, you should assume that any unreadable diskettes are infected, and restore copies from a clean PC as soon as possible.

False alarms

Very occasionally, FindVirus may report a false alarm, that is, it may report a virus in a clean file. This occurs if the pattern of bytes found in a virus is also found in an uninfected file. The chances of a false alarm are increased slightly if you use the `/ANALYSE` option.

If you are in any doubt, contact your authorized distributor or Dr Solomon's Technical Support.

8.4 Error messages

This section gives the most common error messages returned by FindVirus, with an explanation of why the error has occurred.

Cannot execute WFINDV32.EXE

The file cannot be found.

The program has been altered; please replace it with a good copy.

Changes have occurred to WFINDV32.EXE. Copy a clean version of the file from the Toolkit diskette.

Insufficient memory.

There is not enough memory for WFINDV32.EXE to execute.

Bad MESSAGES.DRV

The file MESSAGES.DRV is missing, or it has been altered. Check that the file is in the same folder as WFINDV32.EXE or replace it with a good copy from the original Toolkit diskette.

Bad driver FINDVIRU.DRV

The driver file FINDVIRU.DRV is missing, or it has been altered. Check that the file is in the same folder as WFINDV32.EXE or replace it with a good copy from the original Toolkit diskette.

This program is more than xx months old

FindVirus compares the system date with the date of FINDVIRU.DRV. If the difference is six months or more, FindVirus displays the "out-of-date" message. To ensure you are fully protected from new viruses, you should subscribe to the regular upgrade service. See "Registration and upgrades" on page xiii.

9. Advanced Virus Prevention

This chapter includes detailed information on using VirusGuard, including running the program from the command line or within batch files.

9.1 How VirusGuard works

VirusGuard is a DOS memory-resident program which intercepts viruses, preventing infected files from being executed. It scans each executable file for viruses every time it is opened or executed, and also scans for boot sector and partition sector viruses. If a virus is found, VirusGuard displays a message and sounds an alarm.

VirusGuard consists of three files. GUARD.COM is the memory-resident scanner program, GUARD.DRV is a driver file which contains information on detecting viruses, and MESSAGES.DRV supports messages in different languages.

Running VirusGuard

VirusGuard is best run at system start-up. The Toolkit installation procedure adds GUARD to your AUTOEXEC.BAT file. If you install it separately from the rest of the Toolkit, you should add the appropriate line to the AUTOEXEC.BAT. For example:

```
C:\TOOLKIT\GUARD
```

For increased security, include it as near to the start of the file as possible so VirusGuard is loaded before other software.

If GUARD is not included in your AUTOEXEC.BAT, you must run it from the command line each time you start up the PC.

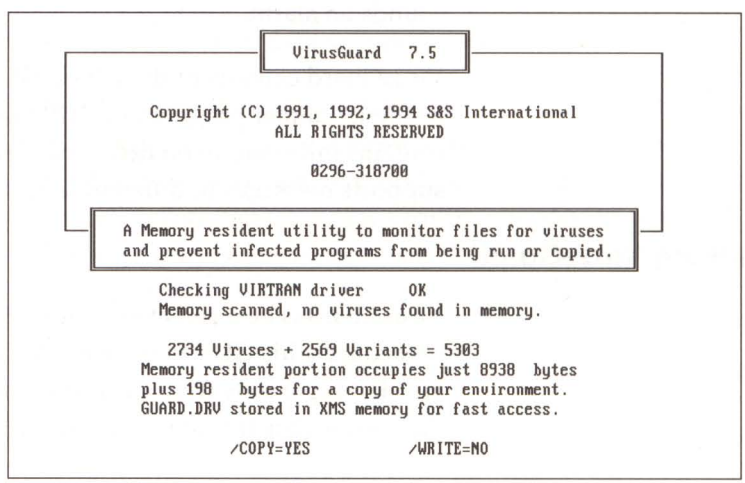
Use of memory

VirusGuard uses about 9 Kb of conventional memory when resident. This is because it only keeps the scanning program permanently in memory, and reads GUARD.DRV from elsewhere.

If your PC has additional memory installed, VirusGuard uses that for storing the driver. It checks for XMS first and if that is unavailable, it looks for EMS. If neither XMS or EMS is available, it accesses the driver from the hard disk.

VirusGuard itself loads in conventional memory. However, you can load VirusGuard high to reduce its need for base memory.

When VirusGuard is loaded, it displays a screen of the following format:


VirusGuard 7.5
Copyright (C) 1991, 1992, 1994 S&S International
ALL RIGHTS RESERVED
0296-318700
A Memory resident utility to monitor files for viruses
and prevent infected programs from being run or copied.
Checking VIRTRAN driver OK
Memory scanned, no viruses found in memory.
2734 Viruses + 2569 Variants = 5303
Memory resident portion occupies just 8938 bytes
plus 198 bytes for a copy of your environment.
GUARD.DRV stored in XMS memory for fast access.
/COPY=YES /WRITE=NO

This screen includes the following information:

- The VirusGuard version number.
- The results of an initial memory scan.
- The number of viruses that VirusGuard currently scans for.
- How much memory GUARD.COM uses.
- Where GUARD.DRV is stored.

- The current settings of the `/WRITE` and `/COPY` switches. (See "Scanning files when copying or reading" on page 101 and "Scanning files when writing" on page 102.)

Security levels

When it is first run, VirusGuard scans the PC's memory, the hard disk's boot and partition sectors, the hidden system files and COMMAND.COM.

You can select one of three different security levels when you install VirusGuard, and subsequent scanning depends on the security level set.

- In its minimum security mode, VirusGuard scans all executable files before they are run. It also scans executable files copied from diskette and scans all diskettes for boot sector viruses.
- In the standard security setting, as well as the minimum scans, VirusGuard scans all executable files as they are copied, not just those that are copied from diskette. This is the default setting.
- In its maximum security mode, VirusGuard additionally scans all files before they are written.

Standard security is adequate for most circumstances. To change the security level at any time after installation, see "Changing the security level" on page 105.

Executable files

File viruses only infect executable files. When scanning executable files, VirusGuard looks for files with the following extensions:

APP	OVL
BIN	OVR
COM	SCR
DLL	SYS
EXE	XTP

Boot sector scans

VirusGuard scans for boot sector viruses whenever you put a diskette into a drive and access it, even if you only run a DIR command. If a boot sector virus is present, VirusGuard will display a warning.

On most PCs, VirusGuard only scans for boot sector viruses the first time you access the diskette. Subsequent accesses are not scanned unless you have removed the diskette and re-inserted it. However, on some 8088 PCs and XTs VirusGuard scans every diskette access.

VirusGuard does not stop you accessing a diskette that is infected with a boot sector virus. The virus can only infect your PC if you try to boot the computer from the infected diskette, so it is safe to copy files from the diskette (assuming that the diskette does not contain any file viruses).

If you leave an infected diskette in the A: drive and reboot the PC, VirusGuard cannot prevent infection, because the virus is loaded from the diskette before VirusGuard is run. VirusGuard warns you when it detects an infected diskette, but it cannot physically stop you using it.

Finding viruses

VirusGuard scans for viruses using the current virus driver. It can find almost all the viruses found by FindVirus. When a virus is found, it will prevent you from running or copying the file in question, and will sound the alarm.

However, there are a few viruses which VirusGuard can detect, but cannot prevent from running. These are some of the more complex polymorphic viruses. If one of these is detected, the pop-up alarm is still displayed. You should immediately run FindVirus to locate and identify the virus and remove it.

9.2 Running VirusGuard

You can run VirusGuard from the command line or within a batch file with a variety of switches and parameters. The standard command syntax is:

```
GUARD [switches]
```

The available switches are discussed in the following sections.

You cannot use any switch more than once on the command line. For example, only the first `/COPY` will have any effect. The switches must be separated by spaces, and they can be typed in upper or lower case.

Scanning files when copying or reading

By default, VirusGuard scans all executable programs when they are copied or read. The `/COPY=` switch can be used to change this default.

```
/COPY=NO
```

Files are not scanned when they are copied or read, only when they are run.

You can also request VirusGuard to scan all files, including data files, whenever they are copied or read.

```
/COPY=ALL
```

Scans all files when they are copied or read, regardless of their extension.

Scanning all files slows down PC performance during disk accesses and makes minimal difference in the level of security, so it is not recommended for general use.

Also, you can specify that VirusGuard should scan files during read and copy operations whenever files are read or copied from local drives.

`/COPY=LOCAL`

Scans files on local drives when they are copied or read.

Alternatively, you can confine read and copy scanning to files that are read or copied from diskette. This gives extra security, particularly since viruses are usually transferred via diskette.

`/COPY=FLOPPY`

Scans files on diskette when they are copied or read.

Scanning files when writing

By default, VirusGuard does not scan files before they are written. You can use the `/WRITE=` switch to change this default.

`/WRITE=YES`

Scans all executable files before they are written.

`/WRITE=ALL`

Scans all files before they are written, regardless of extension.

Scanning all files will slow your PC down during disk accesses and in most circumstances this level of security is unnecessary. You may wish to use this if you have executable files with extensions that would otherwise not be scanned.

You can also restrict VirusGuard to scan files only when they are written to local drives or to diskettes.

`/WRITE=LOCAL`

Scans files on local drives when they are copied or read.

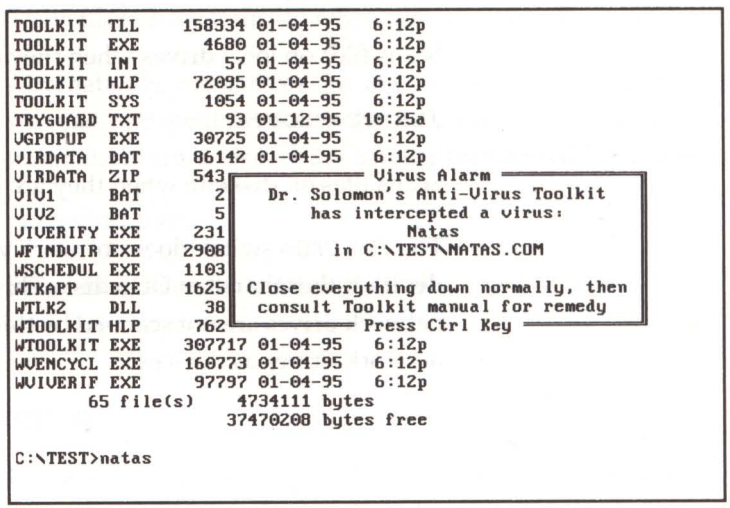
`/WRITE=FLOPPY`

Scans files on diskette when they are copied or read.

The `/WRITE=` switch does not work when a file is written to a device rather than to a DOS disk. This means that files written to network drives are not scanned by this option, because DOS treats network drives as devices.

Changing the pop-up message

The standard VirusGuard alarm box is as follows:



The last line of the message can be changed.

`/WARN="`*`message`*`"` Specifies a particular message to appear on the last line of the pop-up alarm box. The message must be enclosed in quotation marks and can contain any character except double quotation marks (") or forward slash characters (/) to a maximum of 36 characters.

For example:

```
GUARD /WARN="ring 1234"
```

9.3 Hints and Tips

Changing the security level

If you need more or less security at any time, you can change VirusGuard's security level by running `GUARD` with certain switches.

To set VirusGuard to maximum security, use the command:

```
GUARD /COPY=ALL /WRITE=ALL
```

This scans all files when they are copied, read or written.

For standard security, run VirusGuard with no `/COPY` or `/WRITE` switches.

To set VirusGuard to minimum security, use the command:

```
GUARD /COPY=FLOPPY /WRITE=NO
```

This scans for viruses when files are copied and read from diskette. No scanning is performed when files are written.

If GUARD.COM is included in your AUTOEXEC.BAT file, you can edit the parameters using a text editor or a word processor. When you run VirusGuard it confirms the status of the `/COPY` and `/WRITE` switches, as shown on page 98. Virus Guard is not reinstalled.

9.4 Testing VirusGuard

File virus test

To enable you to test VirusGuard and see how it behaves when it detects a file virus, you can set up a test file.

Follow these steps:

1. Before the test, make sure that VirusGuard is loaded and that you do not have the `/COPY=NO` or the `/WRITE=ALL` switches on, as these interfere with the test.

2. Use a text editor or word processor to create a file called `TRYGUARD.DOC`.

3. Enter the first nine characters of the file as:

   ZQZXJVBVT

   These characters must be in upper case.

4. If you want to test FindVirus and WinGuard as well, ensure that there are at least 50 characters in the file.

5. Save the file as an ASCII text file. Do not save it as a formatted document, as this would insert extra characters at the beginning of the file and stop it from being recognized by VirusGuard.

   If VirusGuard is set up with the `/WRITE=ALL` switch, you will not be able to save the file.

6. Rename the file with the following command from the DOS prompt:

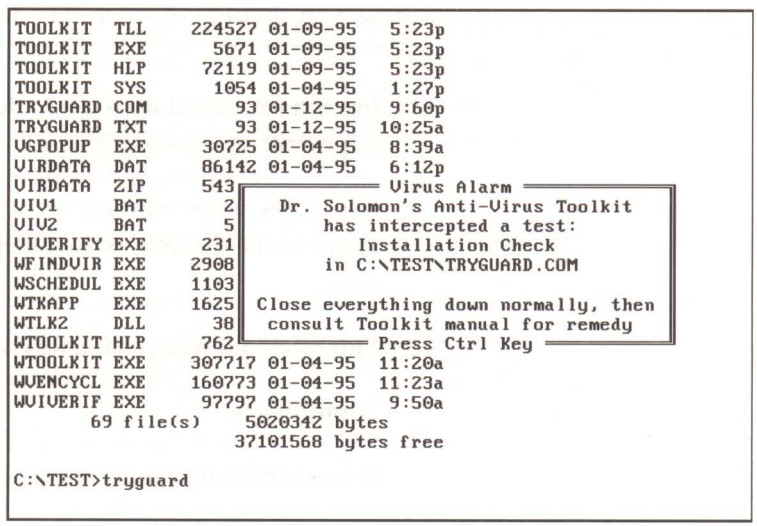
   ```
   REN TRYGUARD.DOC TRYGUARD.COM
   ```

   The COM extension will ensure that VirusGuard scans the file as though it were an executable file.

7. To run the test, enter the command:

```
COPY TRYGUARD.COM NUL
```

DOS attempts to copy the test file, an action which is checked by VirusGuard. The alarm pops up and reports the test as follows:



If the file is at least 50 characters long, it will also be found if you run FindVirus.

VirusGuard would also intercept the file if you tried to run it as a program. However, as the test file is not executable, it would not run even if VirusGuard was not resident, and may cause the PC to hang.

When you have finished the test, delete the file or rename the file giving it a DOC file extension so that FindVirus doesn't give someone a shock later on.

Boot sector virus test

You can perform a similar test on a diskette to see what happens when VirusGuard finds a boot sector virus.

For this test, you need to know how to use a disk sector editor, such as DOS DEBUG. If you are not familiar with tools such as these, you should not attempt to do this.

1. Insert a formatted diskette. Make sure there is nothing important stored on it in case you make a mistake.
2. Use a disk sector editor to write to byte 64 (40H) in the boot sector of the diskette. Remember that the first byte is number zero.
3. Enter the following characters, without the quotation marks:

   "Confidence"

   In hexadecimal, this is:

   43 6F 6E 66 69 64 65 6E 63 65
4. Remove the diskette, then re-insert it and type `DIR` to list the files on the diskette.
5. The VirusGuard pop-up alarm appears, reporting an Installation Check. If you run FindVirus, it will also report the test.

When you have completed the test, reformat the diskette to avoid giving someone a shock later on.

9.5 VirusGuard error messages

This section gives the most common error messages returned by VirusGuard, with an explanation of why the error has occurred.

VirusGuard driver access error! Scan incomplete.

> This message is displayed if VirusGuard is unable to access its driver. Typically, this occurs if VirusGuard has been loaded initially from a network drive which, after login, has been re-mapped so that the directory from which VirusGuard was loaded does not exist.

ERROR - not enough memory to load GUARD.DRV.

> This message is displayed if the PC has XMS or EMS memory, but not enough to store VirusGuard's driver file (GUARD.DRV).

ERROR - Can't find or read GUARD.DRV - VIRUSGUARD NOT INSTALLED.

> GUARD.DRV is not in the same directory from which VirusGuard was loaded; or VirusGuard is unable to read GUARD.DRV.

ERROR - VirusGuard must not be run from a floppy disk. Install the program and drivers on a hard disk and run from there.

> VirusGuard cannot be run from a diskette drive.

CHECKSUM TEST FAILED - TAMPERING DETECTED - VIRUSGUARD NOT INSTALLED.

> GUARD.COM has been altered. Copy a clean version of the file from the Toolkit diskette.

The GUARD.DRV database is xx months old . . . .

VirusGuard compares the system date with the date of GUARD.DRV (the virus driver). If the difference is six months or more, the "out-of-date" message appears.

To ensure you are fully protected from new viruses, you should subscribe to the regular upgrade service. See "Registration and upgrades" on page xiii.

10. Advanced Virus Checking

This chapter provides detailed information on using ViVerify, including running the program from the command line or from within batch files.

10.1 How ViVerify works

ViVerify is a checksummer which is able to detect changes in executable files that may have been caused by a virus infection. ViVerify works by calculating a unique fingerprint for each file. This fingerprint is then recalculated when required, to check if there have been any changes.

Executable files

ViVerify only checks for changes in executable files. By default, it checks files with the following extensions:

APP	FON
BAT	OV?
BIN	SYS
COM	XTP
DLL	386
EXE	

Most executable files do not change, so any variation in the checksum may be an early warning of a virus infection. Occasionally, though, you may have an executable file that does change, or a data file that has one of the above file extensions. Specific individual files of this sort can be excluded from the checks. The following files are excluded by default:

CONFIG.SYS
WPQUE.SYS
WPSYSD.SYS
BOOTCONF.SYS
TELIX.FON

ViVerify also checks boot and partition sectors for changes.

Encryption algorithms

To create unique fingerprints (checksums) which cannot be detected by the virus, ViVerify uses an encryption algorithm.

The default algorithm used is the CCITT Cyclic Redundancy Check (CRC). This incorporates a user-specified keyword to increase security, and checks the files rapidly.

The Size algorithm calculates fingerprints based only on the size of the file. This is very quick, but can be fooled, or "spoofed", by some viruses.

The Checksum algorithm calculates fingerprints as a whole sum of the bytes checked in the files. It also incorporates the user-specified keyword.

The DES algorithm uses the standard Data Encryption Standard (DES) algorithm. This is the most secure option, but requires lengthy calculations, so it can slow down the checking.

Checking speed

By default, ViVerify speeds up the checking process by checking only the first and last 4 Kb of each file. This is known as turbo mode. If you need particularly high security, you can turn turbo mode off, allowing ViVerify to check the entire file.

However, it is very unlikely that a virus will infect a file without making changes to the beginning or end of the file.

To speed up checking further, ViVerify normally checks only every fifth byte in a file since it is difficult for a virus to infect a file without modifying at least one of the bytes checked by ViVerify. You can change this if you need greater security or faster checking on your system.

Running ViVerify

There are two stages to running ViVerify:

- Calculating the fingerprints of the files to be checked for changes.
- When required, recalculating the fingerprints to check for changes.

10.2 Running ViVerify from the user interface

You can run ViVerify from the Toolkit user interface in the following ways:

- By selecting the Check for Changes option on the main screen.
- By selecting Check for Changes from the Scan menu.

These options are explained in detail in Chapter 5. See "Checking for changes - ViVerify" on page 49.

10.3 Running ViVerify from the command line

You can run ViVerify directly from the command line by clicking on Start, selecting the Run option and typing the command in response to the Open: prompt. You can also include the appropriate commands within a batch file.

Syntax

The standard command syntax is:

```
V2WIN32 [switches]
```

The available switches are as follows:

Switch	Meaning
/BEEP	Beep when a changed file is encountered.
/CRC	Use the CCITT Cyclic Redundancy Check algorithm (default).
/CREATE	Create a file containing a list of files and their calculated fingerprints.
/D=	Specify the drive(s) to be checked.
/DES	Use the DES algorithm.
/FS=*file* /FPRINT=*file*	Define file holding the fingerprints.
/LOUD	Display status of each file checked.
/N=n	Check every nth byte of each file.
/NETVOL	Exclude unreadable network files from a file list.
/NT	Do not use turbo mode; check entire contents of file.
/PRINTOUT	Output report to printer as well as to screen.
/REPORT=*file*	Output report to specified file as well as screen.
/SIZES	Use the file size algorithm.
/WHOLESUM	Use the whole sum algorithm.
/X=*keyword*	Specify the keyword to be used.

The available switches are explained in detail in the following sections. You cannot use any switch more than once on the command line. The switches must be separated by spaces, and they can be typed in upper or lower case.

Checking specific drives

When using any function, you should specify the drive(s) to be checked using the /D= switch.

`/D=drive` Indicates one or more drives to be checked.

Enter one or more of the identifying letters, each one with its colon and with semicolons as separators. For example:

```
V2WIN32 /D=C:;D:
```

will check the C: and D: drives.

Defining drives to be checked

By default, ViVerify checks all executable files on the selected drive. When you use the CREATE switch, it will create a file containing the fingerprints of all the files to be checked.

If you want to check the contents of different drives separately, you can create a separate fingerprint file for each drive. In these circumstances, you should define particular file lists to be used, rather than using the default filename.

`/FS=file` With the /CREATE switch, creates a file containing the fingerprints of all executable files on the drive(s). Without the /CREATE switch, checks all executable files in the fingerprint file.

For example:

```
V2WIN32 /D=C: /FS=C_FILES.VVF /create
```

creates a file containing the fingerprints of all executable files on the C drive, with the filename C_FILES.VVF.

Specifying a fingerprint file

If you want to check the contents of various folders separately, you can create a separate fingerprint file for each folder. For example:

V2WIN32 /D=C:\TOOLKIT /FS=C_FILES.VVF /CREATE

Remember that when you subsequently check the fingerprints you must use the same file that you specified when you created the fingerprints.

Checking files

By running ViVerify without the /CREATE switch you use the fingerprint file already created to check if any executable files have changed..

Checking boot and partition sectors

By default, ViVerify checks the boot and partition sectors of every disk it examines. You can turn these checks off, but this is not recommended unless an option is causing a problem. For example, if you are checking a network drive which does not have a boot sector.

`/NOBOOT`	Stops ViVerify from checking the boot sectors.
`/NOPART`	Stops ViVerify from checking partition sectors.

Specifying a keyword

When you use the /CREATE switch, you must specify a keyword to be used in the fingerprinting algorithm.

When you subsequently check the same list of files, you must give the same keyword as a parameter.

`/X=keyword` Specifies a keyword to be used when creating or checking fingerprints. The keyword must be at least eight alpha-numeric characters.

For example:

```
V2WIN32 /D=C: /X=D5R2L0H7
```

will create a list of executable files on the C drive to be checked, and will create fingerprints for these listed files, incorporating the user-specified keyword.

Varying the checking speed and security

If you need a particularly high level of security, you can turn off turbo mode, forcing ViVerify to check the entire file instead of just the first and last 4 Kb.

`/NT` Turns off turbo mode.

ViVerify normally checks every fifth byte in each file, which is sufficient for most users. You can set the program up to check more bytes, to provide greater security, or fewer bytes, for faster checking.

`/N=n` Checks every nth byte in each file.

Specifying an algorithm

By default, ViVerify calculates fingerprints using the CCITT Cyclic Redundancy Check algorithm. This is suitable for most users, but you can specify a different algorithm if you specifically need greater security or increased checking speed.

`/SIZES` Calculates fingerprints based on the file size.

`/CRC` Uses the CCITT CRC algorithm (default).

`/WHOLESUM` Calculates fingerprints as a whole sum of the bytes checked in the file.

`/DES`	Uses the Data Encryption Standard algorithm.

Defining actions

You can configure ViVerify to beep when it finds a changed file.

`/BEEP`	Beep when a changed file is found.
`/BIGBEEP`	Beep loudly when a changed file is found

Producing reports

You can direct the report to a named file, to the default system printer or to both. You can specify whether the output appears in full or in a shortened form.

`/PRINTOUT`	Directs the report to the default system printer as well as to the screen.
`/REPORT=`*`file`*	Directs the report to the specified file as well as to the screen.
`/LOUD`	Provides a more detailed report. As each file is checked, its name is displayed on the screen.
`/QUIET`	Produces a report in a shortened form.

For example:

```
V2WIN32 /D=C: /X=D5R2L0H7 /PRINTOUT /LOUD
```

will recalculate fingerprints for executable files on the C drive, using the specified keyword in the encryption algorithm. As each file is checked for changes, its name is displayed on the screen, and the report is also sent to the default printer.

11. Toolkit Configuration

This chapter explains the configuration files which are used within the Toolkit.

11.1 The TOOLKIT.INI file

The TOOLKIT.INI file is used to hold a number of settings for the Toolkit programs. It is loaded automatically when you start the Toolkit. You can edit this file to customize it to your own installation, and you can create other files for different configurations, for example, for different users.

The file is divided into subsections, each of which starts with a heading in square brackets. Beneath each subsection is a list of options defining the current settings.

An example of the TOOLKIT.INI file is as follows:

```
[FindVirus]
Options=BEEP
Report=TOOLKIT.LST
List=FILES.VVL

[FileRepair]
Options=DELETE

[ViVerify]
Options=FILELIST SIZES
Report=VERIFY.REP
FPrint=FINGERP.VVF
```

Note the following points about the format of the file:

- Do not include spaces.
- Where filenames are included, files are assumed to be in the standard Toolkit folder (default C:\TOOLKIT) unless you give a full pathname.

The options that can be included are described below.

FindVirus

`Options=switches`	These can be any of the command line switches available for the WFINDV32 command. Do not include the slash character. Options containing an equals sign must be placed on separate lines.
`Report=`*`file`*	The output report file.
`List=`*`file`*	The file containing the list of files to be scanned.
`Driver=`*`file`*	The driver file to be used.

For more information on the available switches, see Chapter 8, "Advanced Virus Detection".

FileRepair

When FindVirus is run with the file repair option, it always tries to repair an infected file. If the file cannot be repaired, the file can either be renamed or deleted.

`Options=`	If you wish to rename files that cannot be repaired, specify RENAME. If you wish to delete files that cannot be repaired, specify DELETE.

ViVerify

`Options=switches`	Include any of the V2WIN32 command line switches. Do not include the slash character. Options containing an equals sign must be placed on separate lines.
`Report=`*`file`*	The output report file.
`Fprint=`*`file`*	The file containing the list of fingerprints.

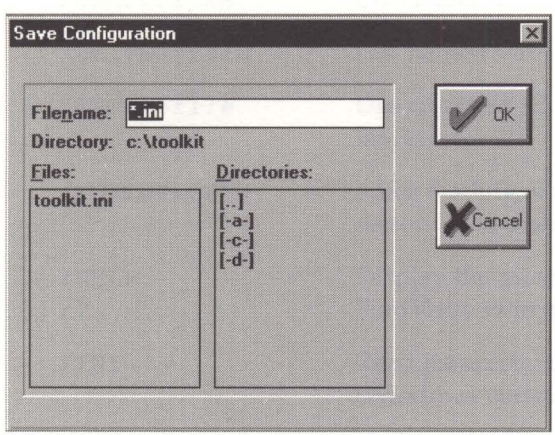
For more information on the available switches, see Chapter 10, "Advanced Virus Checking".

11.2 Configuration File Management

You can edit TOOLKIT.INI using any text editor or word processor that can save the file as unformatted ASCII text.

Alternatively, you can load and save the configuration details held in TOOLKIT.INI from the user interface.

When you have set up a specific set of defaults for FindVirus and ViVerify you can save the settings in a configuration file. Select Save Configuration from the File menu. A file selector box of the following format is displayed:



Provide a name for the file to be saved, and select OK.

By default, the Toolkit loads TOOLKIT.INI when it starts up. To reload a different configuration file, containing previously saved settings, select Load Configuration from the File menu. Select or enter the name of the file to be saved and select OK. The file is loaded and the new settings are applied.

12.Reference Information

This chapter includes reference information, including the command line syntax and switches for all the Toolkit commands.

12.1 FINDVIRU command

Syntax

```
FINDVIRU [switches]
```

Switches

Switch	Meaning
/ALLDRIVES	Check all fixed disk drives, including network drives.
/BADLIST=*file*	Write suspect filenames to the specified file.
/BEEP	Beep when a virus is found.
/CHECKLIST=*file*	Check files listed in specified file.
/D=drives	Check specified drives.
/DOALLFILES	Check all files, not just executables.
/DRIVER=*file*	Use named virus driver file.
/EXTRA=*file*	Use specified additional virus driver.
/FORCEFLOPPY	Force reading of diskette boot sector when diskette is changed.
/HELP /?	Display the most common FindVirus switches.
/INI	Read parameters from INI file (Windows version only).
/LOCAL	Check local hard disk drives.

Switch	Meaning
`/LOUD`	Display status of each file scanned.
`/NOBOOT`	Do not scan boot or partition sector.
`/NOFILES`	Disable file scanning.
`/NOPACK`	Do not scan files compressed with PKLite and LZExe.
`/NOPART`	Do not check partition sectors.
`/ONEONLY`	Check one diskette only.
`/ONVIRUS=HALT` `/ONVIRUS="`*`msg`*`"`	Carry out the specified action if a virus is found.
`/PACK`	Scan files compressed with PKLite, LZExe, ICE, DIET or CRYPTCOM.
`/PAUSE`	Pause for keystroke before scanning.
`/PRINTOUT`	Output report to the printer as well as to the screen.
`/REPAIR[/DELETE]`	Repair infected files. The optional `/DELETE` switch deletes files that cannot be repaired.
`/REPORT=`*`file`*	Output report to specified file.
`/SILENT`	Suppress screen output.
`/SUMMARY`	Produce a summary report.
`/UNPACK`	Scan compressed files. (Superseded by `/UNZIP` and `/PACK`.)
`/UNZIP`	Scan files compressed with PKZIP, ARJ, PKLite, LZExe, PKARC, ICE, DIET, LHA or CRYPTCOM.
`/YESBREAK`	Enable interruption with Ctrl Break.

12.2 GUARD command

Syntax

```
GUARD [switches]
```

Switches

Switch	Meaning
/COPY=NO /COPY=YES /COPY=FLOPPY /COPY=LOCAL /COPY=ALL	Define whether or not files are to be scanned when they are copied and read.
/CODE="*code*"	Check diskettes for authorisation code.
/FON	Scan Windows font files.
/MODE=EMS	Force use of EMS memory.
/MODE=DISK	Force use of hard disk.
/REGUARD	Reactivate VirusGuard.
/STRICT	Prevent access to unauthorised diskettes. Must be used with the /CODE switch.
/WARN="*message*"	Display a warning message.
/WRITE=NO /WRITE=YES /WRITE=FLOPPY /WRITE=LOCAL /WRITE=ALL	Define whether or not files are to be scanned when they are written.

12.3 VIVERIFY command

Syntax

```
VIVERIFY [switches]
```

Switches

Switch	Meaning
/ASM	Use Anti-Stealth Methodology.
/BADLIST	Create a list of files that have changed.
/BEEP	Beep when a changed file is encountered.
/CRC	Use the CCITT Cyclic Redundancy Check algorithm (default).
/D=	Specify the drive(s) to be checked.
/DES	Use the DES algorithm.
/FS=*file* /FPRINT=*file*	Define file holding the fingerprints.
/LOUD	Display status of each file checked.
/N=n	Check every nth byte of each file.
/NETVOL	Exclude unreadable network files from a file list.
/NOBOOT	Do not check boot sector.
/NOPART	Do not check partition sector.
/NT	Do not use turbo mode; check entire contents of file.
/PRINTOUT	Output report to printer as well as to screen.
/REPORT=*file*	Output report to specified file as well as screen.

Switch	Meaning
/SIZES	Use the file size algorithm.
/WHOLESUM	Use the whole sum algorithm.
/X=*keyword*	Specify the keyword to be used.

12.4 CLEANBOO command

Syntax

CLEANBOO [*drive*] [/*type*] [/NOASM]

where:

drive	is the drive containing the diskette to be repaired.
type	is a number between 1 and 5 or the letter A, to indicate the diskette type.

Switches

Switch	Meaning
/NOASM	Disable Anti-Stealth Methodology

12.5 WTKUTIL command

Syntax

```
WTKUTIL [switches] COMMAND [switches] [optional
parameters ...] switches
```

Switches

Switch	Meaning
`/help or /?`	display help, then continue with valid commands, if any

Commands

ADD

```
WTKUTIL ADD WINGUARD toolkitpath
```

Modify WIN.INI and the registry to enable WinGuard next time the PC in rebooted. WinGuard must be in the specified path.

REMOVE

```
WTKUTIL REMOVE WINGUARD
```

Modify WIN.INI and the registry to disable WinGuard next time the PC in rebooted.

WINGUARDCHECK

```
WTKUTIL WINGUARDCHECK
```

Display a message indicating whether or not WinGuard is loaded. Return error level 1 if WinGuard is loaded, error level 2 otherwise.

SAVESETTINGS

```
WTKUTIL SAVESETTINGS WINGUARD filename
```

Write WinGuard's settings to the specified file, in text format. Return error level 255 if the file or registry section cannot be opened, error level 0 for a successful operation.

LOADSETTINGS

```
WTKUTIL LOADSETTINGS WINGUARD filename
```

Delete the current WinGuard settings and replace them with those read from the specified file. Return error level 255 if the file cannot be opened, error level 0 for a successful operation. (This command does not enable WinGuard.)

CHECKSETTINGS

```
WTKUTIL CHECKSETTINGS WINGUARD filename
```

Compare WinGuard's current settings with those stored in the specified file. Return error level 1 if the settings are the same, error level 2 if they are different, error level 255 if the file or registry section cannot be opened.

This page has been left blank.

Glossary

alias	A different name by which a *virus* is known.
AUTOEXEC.BAT	This file is run whenever you boot your PC.
backup	A copy of your data held in another place in case your working copy is lost or damaged.
batch program	A file containing a set of commands that you can run by typing just one command. Batch files have the file extension BAT.
BBS	Bulletin Board System. An electronic mail system used to send messages and transfer files.
BIOS	Basic Input/Output System. Permanent programs that are used to load the operating system when the system is started up.
boot	Start the computer.
boot diskette	A diskette containing operating system files which can be used to start up your computer.
boot sector	The part of every hard disk and diskette that is read by the computer when it starts up.
boot sector virus	A virus transmitted in the *boot sector* of a diskette. Boot sector viruses infect the boot sectors of hard disks, and often the *partition sectors* as well.

bug	An unintentional fault in a program.
CARO	Computer Anti-Virus Researchers Organization. Several S&S staff are members of CARO.
checksummer	A program that looks for viruses by checking for changes in *executable files*. ViVerify is an example of a checksummer.
clean	Free from viruses.
COM file	An *executable file* with a file extension of COM.
CONFIG.SYS	This file is run whenever you boot your PC.
defragmenters	A program which reorganizes a hard disk so that different *clusters* of each file are stored contiguously if possible. This improves disk efficiency.
device driver	A program used to control the items of hardware connected to the PC such as disk drives and printers. .
directory	see 'Folder'.
disk compressor	A program which stores files in a compressed form to maximize space on the hard disk.
dropper	A file which is not itself a virus, but infects the PC.
driver file	A file used by the Toolkit to enable the identification and reporting of viruses.

EICAR	European Institute for Computer Anti-Virus Research. S&S International is a member of EICAR.
EXE file	An *executable file* with the file extension EXE.
executable file	A file containing a program which can be run by typing its filename at the DOS command line or by clicking on its name in the program list displayed by Explorer.
false alarm	A report of a virus where none exists.
fast infectors	A file virus that infects programs when they are opened or copied as well as when they are run.
file virus	A virus which infects *executable files*. When the program is run the virus copies itself. Most file viruses are *memory resident*.
fingerprint	A unique numeric identifier for a file; used by *checksummers* to check for changes in executable files. Also known as a checksum.
folder	A logical subdivision of a disk which organizes files into groups.
footbath PC	A PC used to check incoming files and diskettes for viruses. Also known as a *sheep-dip* PC.
format	The method of preparing a disk before files are written to it, using the FORMAT command.

GDE	Generic Decryption Engine. An element of FindVirus which enables it to identify even the most complex polymorphic encrypted viruses.
hexadecimal	Representation in base 16.
heuristic scanner	An element of FindVirus which checks files for suspicious code which may indicate a new virus.
infected file	A file containing a virus.
joke programs	Practical joke programs. These are not viruses, but sometimes a virus is contained in a joke program. The Toolkit detects joke programs.
logic bombs	A type of *trojan* that is triggered by a particular set of circumstances.
macro file	A data file containing instructions that specify actions to be taken by an applications program.
Master Boot Record	The partition sector of a hard disk.
memory resident	A program which remains in the PC's memory once it has run. Also known as *TSR* or *VxD*.
multi-partite virus	A virus which uses a combination of techniques to spread, for example, infecting both files and *boot sectors*.
overwriting virus	A virus which overwrites each file it infects.
partition sector	The first part of a hard disk to be read. This contains the location of each partition, and the number of sectors in each one.

partition sector virus	A virus that replaces the normal *partition sector* of a hard disk.
polymorphic virus	A virus that tries to evade detection by scanners by ensuring that it does not have a fixed pattern of bytes. The Toolkit can detect polymorphic viruses using the Generic Decryption Engine.
public domain software	Software which you can copy and distribute legally.
root folder	The topmost folder on a disk, where all other folders and files are stored.
scanner	A virus detection program that searches for viruses. FindVirus is an example of a scanner.
shareware	Software which you can copy legally, but must pay for if you decide to use it.
sheep-dip PC	A PC used to check incoming files and diskettes for viruses. Sometimes called a footbath PC.
stealth	Characteristic of a virus which tries to avoid detection. Stealth viruses interfere with DOS and *BIOS interrupts* in order to conceal their presence.
SYS file	File, generally a *device driver*, with an extension of SYS.
time bombs	A type of *trojan* that is triggered by a particular date.
trojan	A program that has an unexpected action. Trojans are not viruses, as they do not replicate, but they are often

	damaging and are detected by the Toolkit.
TSR	Terminate and Stay Resident. A DOS program that remains in memory after it has run. See *memory-resident*.
upgrade	A new version of the Toolkit which has been updated to detect newly-discovered viruses. Upgrades are available quarterly or monthly.
variant	A variation of a virus, usually caused by amending the code of an existing virus.
virus	A program that replicates itself.
VxD	Virtual device driver. A Windows program that remains in memory after it has run. See *memory-resident*.
write-protect	Ensuring that files cannot be written to a disk. A 5¼" diskette is write- protected by placing a label over the notch. A 3½" diskette is write-protected by sliding a plastic tab to uncover a hole.

Index

A
Advanced menu 30
algorithm 55, 117
aliases 7
anti-virus policy 11
archived files 42, 76, 84, 90
ARJ 42, 76, 84, 90
AUTOEXEC.BAT 97
autoloader 68

B
backup diskettes 95
backups 10, 11, 17
boot sector
    explanation 4
    FindVirus checks 91
    replacing 4, 60, 61, 62, 65, 66
    virus 4
    VirusGuard checks 100
    ViVerify checks 116
bugs 8
bulletin boards 8, 12

C
CARO 7
changed files 53
Check for Changes menu option 29
Checksum algorithm 55, 112
checksummers 13, 111
checksums 14, 49
CLEANBOO command
    switches 127, 128
    syntax 127, 128
clean-up operation 68
closing the Toolkit 28
CMOS 12
companion virus 5
compressed files 42, 75, 84, 90
Computer Anti-Virus Researchers Organisation 7
configuration file management 121
configuration files 44, 56, 119
conventional memory 98
conventions ix
CRC algorithm 55, 112, 117
Cyclic Redundancy Check. See CRC algorithm

D
Data Encryption Standard. See DES
deleting files 65, 67
DES algorithm 55, 112, 118
disable event 72
disk sector editor 108
disk space ix, 18
diskettes 7, 12, 65
DOS Toolkit x, 60
downloading software 12
Dr Solomon's contact details xiv
dropper 6

E
EMS. See expanded memory
enable event 72
encrypted files 85
encryption algorithm 112
eradicating a virus 68
event
    description 71
    disable 78
    editing 78
    enabling 78
    validating 78
event file 78
event log 79
executable files 84, 99, 111
Exit menu option 29
expanded memory 37, 98
extended memory 37, 98
EXTRA.DRV 93

F
false alarms 95
File menu 28
file virus 3
Find Viruses menu option 29
FINDVIRU command
    switches 123
    syntax 123
FindVirus
    advanced menu options 45

command syntax 86
configuration file 120
driver file 93
error messages 95
executable files 84
how it works 83
purpose 13, 14, 31, 39
repairing files 85
reporting 41, 91
running from the command line 86
running from the main screen 40
running from the user interface 41, 86
scanning specific drives 88
scanning specific files 89
Scheduler settings 75
switches 86
testing 106
when to use 39
fingerprint 14, 49, 54, 111, 112

G
games 8, 13
Generic Decryption Engine 7
GUARD command
adding to AUTOEXEC.BAT 97
switches 101–??, 125
syntax 101, 125
GUARD.COM 97
GUARD.DRV 97

H
hardware requirements ix
help text 72
heuristic scanner 13, 92
Heuristic scanning 76
human error 10

I
installation
Scheduler 19, 21
Toolkit 17
upgrades 24
installing the Toolkit 17

J
joke programs 10

K
keyboard 52
keyword 49, 116

L
Load Configuration menu option 28
loading configuration file 122
logic bomb 10
low-level programs 9
LZExe 42, 65, 76, 90

M
main screen 27, 40
Master Boot Record 4
MEM command 37
MESSAGES.DRV 97
multipartite virus 5

N
network
drive 38
virus infection 8
new virus 13, 62
Novell NetWare xii

O
OS/2 xii
overwriting virus 5

P
partition sector
explanation 4
FindVirus checks 91
ViVerify checks 116
partition sector viruses 4
pirated software 12
PKLite 42, 65, 76, 90
PKZIP 42, 76, 84, 90
polymorphism 6
pop-up alarm 36, 38

R
RAM drive 38
README files xiv, 9, 23, 24
reference information 123
registration xiii
renaming files 61, 65
Repair File menu option 29
Repair menu 29, 64
repairing
files 64, 85, 94

from user interface 61
single button 61
Replace Boot Sector menu option 29
replacing boot sectors 4, 60, 61, 62, 65
running an application 74

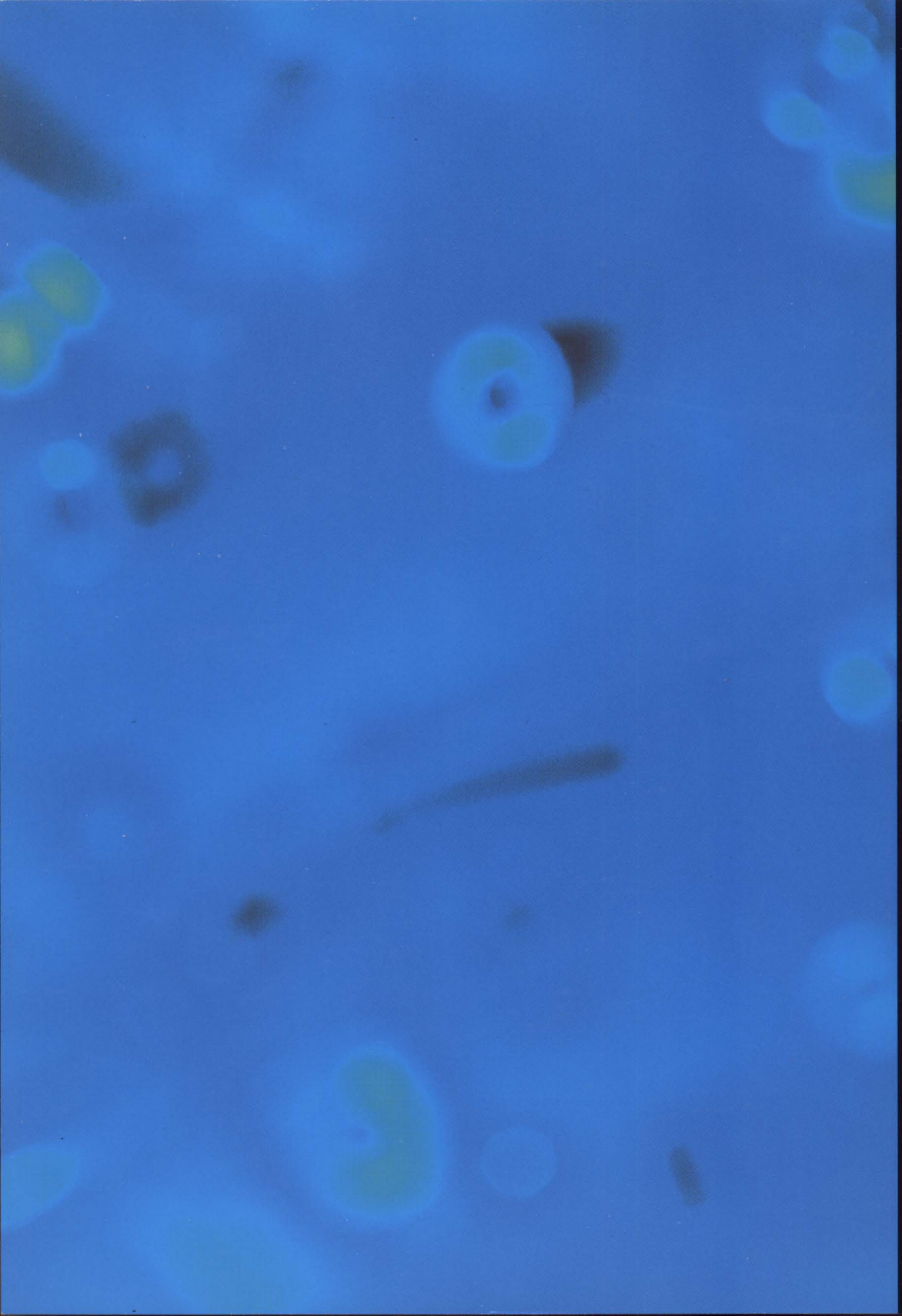
S
save configuration file 121
Save Configuration menu option 28
Scan menu 29
scanners 13
scanning specific files 90
Schedule Editor 71
Schedule menu option 30
Scheduler
adding an event 73
defaults 79
frequency settings 77
installation 21
list boxes 82
running 78
scan settings 81
security levels 105
shareware 8, 82
sheep-dip PC 14, 85
short-cut keys x
Shred
menu option 29
running from the user interface 67
single-button repair 61, 65
Size algorithm 55, 112, 117
software requirements ix
software sources 12
sounding the alarm 36, 38
spoofing 49, 112
status bar 79
stealth 6
Support contact points xiv

T
technical support xiv, 23, 63, 95
test file 106
testing FindVirus 106
testing VirusGuard 106
time bomb 10
toolbar 26, 72
Toolkit
configuration 119
other versions xii
program group 25
TOOLKIT.INI
editing 121
example 119
explanation 119
tooltips 79
trojans 9
turbo mode 56, 112, 117

U
uninstalling 23
unrepairable files 61
upgrades xiii, 24, 96, 110
user interface 27

V
V2WIN32 command
functions 113
syntax 113
variants 7
virus
characteristics 6
definition 1
names 7
new 62
prevention 11
reporting 59
side effects 2
types 3
Virus Encyclopaedia xi, 6, 15, 26, 56
Virus Encyclopaedia menu option 30
VirusGuard
error messages 109
executable files 20, 99
hints and tips 105
how it works 97
reporting 36, 38
running 97, 101
security levels 99
switches 101–??
testing 106
use of memory 98
ViVerify
advanced menu options 54
algorithms 55, 112, 117
checking speed 112, 117
command line switches 114
computing fingerprints 51, 52
configuration file 121

executable files 111
how it works 111
keyword 51, 116
purpose 14, 49
reporting 50, 118
running from the command line 113
running from the user interface 50, 113
verifying fingerprints 51, 53
when to use 50
VIVERIFY command
switches 114, 126
syntax 126

W
WFINDV32 command
switches 86
syntax 86
Windows icons 25
Windows Startup group 21, 78
WinGuard 32

X
XMS. See extended memory